

LIBRARY OF CONGRESS
UNITED STATES COPYRIGHT OFFICE
SIXTH TRIENNIAL 1201 RULEMAKING HEARINGS
Tuesday, May 26, 2015
Library of Congress
Mumford Room
Washington, D.C.

Reported by: Christine Allen,
Capital Reporting Company

1 A P P E A R A N C E S

2 JACQUELINE CHARLESWORTH,
U.S. Copyright Office

3 MICHELLE CHOE,
4 U.S. Copyright Office

5 REGAN SMITH,
U.S. Copyright Office

6 SY DAMLE,
7 U.S. Copyright Office

8 STEVE RUWE,
U.S. Copyright Office

9 JOHN RILEY,
10 U.S. Copyright Office

11 STACY CHENEY,
U.S. Department of Commerce

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1	C O N T E N T S	
2		PAGE
3	Proposed Class 25 - Software-Security Research	4
4	Proposed Class 11-12 - Unlocking - Wireless	
5	Telephone Handsets and	
6	Tablets	206
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		

1 P R O C E E D I N G S

2 MS. CHARLESWORTH: Good morning,
3 everyone. I'm sorry for that brief delay. We were
4 working on an exhibit issue, as I mentioned.

5 Welcome to the Sixth Triennial Section
6 1201 Rulemaking. I'm happy to see we have so many
7 here with us today.

8 I'm Jacqueline Charlesworth, General
9 Counsel of the U.S. Copyright Office, and I and my
10 colleagues -- with my colleagues will be presiding
11 over the hearing -- hearings here in Washington.

12 We had hearings last week which were very
13 productive, and I'm looking forward to another
14 week of hearings here that will be equally as
15 productive.

16 I am joined here, as I mentioned, by
17 several colleagues. I think I'll just go -- have
18 them introduce themselves and say what their title
19 is, starting with Michelle Choe.

20 MS. CHOE: Hi. I'm Michelle Choe. I'm a
21 Ringer fellow at the U.S. Copyright Office.

22 MS. SMITH: Regan Smith, Assistant
23 General Counsel.

24 MR. DAMLE: I'm Sy Damle. I'm Deputy
25 General Counsel.

1 MR. RUWE: Steve Ruwe, Assistant General
2 Counsel.

3 MR. RILEY: John Riley, Attorney-
4 Advisor.

5 MR. CHENEY: And I'm Stacy Cheney. I'm
6 a Senior Attorney at NTIA, Department of Commerce.

7 MS. CHARLESWORTH: Okay. So you have a
8 large audience here. We're all very interested in
9 what you have to say.

10 As I mentioned in Los Angeles, and I'll
11 say it again today, the goal of the hearing
12 process is really to clarify and amplify the
13 record especially in areas where we have
14 questions.

15 And so in making your comments and
16 contributions today, it's helpful if you hone in
17 on the areas of controversy, the sort of disputed
18 areas rather than just sort of restating things
19 that you've said in your written comments, which
20 we've all read and -- carefully and digested.

21 So the format we're going to use is I'll
22 go around -- we have quite a number of
23 participants today -- ask for a brief opening
24 statement that, again, sort of focuses on sort of
25 what you think the key issues in the proposal are,

1 maybe responding to the other side a bit.

2 And we do sometimes interrupt with
3 questions. So be prepared.

4 And, you know, this -- we found that
5 that worked well. And basically our goal is to
6 kind of join the issues. We're particularly
7 interested, especially in a very broad class like
8 this, in how we might refine and kind of define
9 what it is that's being proposed and, you know,
10 looking at that in relation to the support in the
11 record.

12 So just a few rules of the road. We
13 have a court reporter who will, I think, speak up
14 if she can't hear you. For her sake, let's try
15 not to talk over one another.

16 The miking system, as I understand it,
17 only allows four mikes to be on at a time. So as
18 we came from L.A. -- we didn't have that issue in
19 Los Angeles, but we have it here.

20 So the safest thing to do -- obviously,
21 some of you are sharing mikes. Just turn them off
22 when you're not speaking. And somewhat
23 counterintuitively, red means on and white means
24 off. This is a brain test, the mike system.

25 If you want to contribute to the

1 conversation, tip up your placard, and we will
2 call on you as best we can. We try to get to
3 everyone. Sometimes we're a little out of order
4 because I don't see everyone. But we will -- we
5 do try to get all the comments in.

6 And in terms of -- if you're referring
7 to a particular piece of evidence in the record,
8 if it was submitted with your written comments --
9 say, multimedia evidence -- it helps if you can be
10 very specific of what you're referring to.

11 I think we have one -- just one exhibit
12 today, right, that we've premarked. So that would
13 be Exhibit 10. And when we get to that, if you
14 can refer to it as Exhibit 10 just for the record
15 because, when we go back through, sometimes it's
16 hard to sort out what's what.

17 So without further ado, I'm going to ask
18 you each to introduce yourself and just -- just go
19 around quickly. Introduce yourself, explaining
20 what your affiliation is or what interest you
21 represent. And then we'll start again from left
22 to right, and we'll have you make your brief
23 opening statements.

24 So we'll start with you, Professor
25 Green.

1 MR. GREEN: My name is Matthew Green.

2 I'm a professor at Johns Hopkins, and I am one of
3 the petitioners here today.

4 (Microphone interference.)

5 MS. CHARLESWORTH: What's that? It was
6 not good.

7 How is your mike? Is your mike doing
8 that, Mr. Reid?

9 MR. REID: It doesn't seem that way.

10 MS. CHARLESWORTH: Okay. So what I'm
11 going to ask is that -- if you guys could share
12 Mr. Reid's mike, and we'll take that one out of
13 service.

14 MR. REID: Blake Reid, from the
15 Samuelson-Glushko Technology Law and Policy Clinic
16 at the University of Colorado.

17 MR. SAYLER: Andy Sayler, also from the
18 Samuelson-Glushko Tech Law and Policy Clinic at
19 University of Colorado.

20 MR. STANISLAV: Mark Stanislav From
21 Rapid7.

22 MR. BELLOVIN: Steven Bellovin, a
23 professor at Columbia University.

24 MS. MATWYSHYN: I'm Andrea Matwyshyn
25 from Princeton University. I'm representing the

1 security researchers, and I'm also here in my
2 capacity as a law professor.

3 MR. BLAZE: I'm Matt Blaze. I am a
4 professor in the computer science department at
5 the University of Pennsylvania.

6 MS. MOY: Hi. I'm Laura Moy. I'm
7 senior policy counsel at New America's Open
8 Technology Institute.

9 MR. STALLMAN: Hi. Erik Stallman from
10 the Center for Democracy and Technology, here in
11 support of the petitioners.

12 MR. TRONCOSO: Hi. Christian Troncoso
13 with BSA, the Software Alliance.

14 MR. LIGHTSEY: I'm Harry Lightsey with
15 General Motors. And by way of introduction, to my
16 immediate left is Anna Shaw. She's counsel for
17 General Motors with Hogan and Lovells. She will
18 not be providing any testimony or remarks in
19 today's proceeding.

20 MS. CHARLESWORTH: Okay. Thank you.
21 Thank you very much.

22 Professor Green, do you want to lead us
23 off, then?

24 MR. GREEN: Okay. So my name is Matthew
25 Green. I'm a professor of computer science at

1 Johns Hopkins, as I just said. My research is in
2 the area of computer security and applied
3 cryptography.

4 While I'm currently a professor, my
5 career has spanned both academia and industry.
6 Before I became a professor, I was a professional
7 security researcher. I worked for companies such
8 as MasterCard and the Walt Disney Company to find
9 and close vulnerabilities in computer security
10 systems before somebody else could exploit them
11 for commercial gain.

12 Today, as a university professional, I
13 do essentially the same thing, only now my clients
14 are the general public. In both cases, the goal
15 is the same. It's to find flaws in systems and to
16 get them repaired before they can be exploited by
17 somebody else.

18 One of the common themes in my career is
19 risk and finding ways to mitigate risk. I'm not
20 speaking here of only the risk caused by security
21 vulnerabilities, although that risk is real and is
22 increasing. I'm also speaking of the legal risk
23 that security researchers such as myself and my
24 colleagues here today face when they undertake
25 good-faith security research into information

1 security systems.

2 My first exposure to this risk came
3 several years ago when I was a graduate student.
4 More than a decade ago, my colleagues and I
5 discovered serious vulnerabilities in a computer
6 chip that was used to operate in one of the
7 largest wireless payment systems at the time and
8 also to implement the automotive security systems
9 that kept people from stealing cars.

10 The project was the first public
11 security research project that I had conducted at
12 that time. And I have to admit that I was young
13 and I was a bit naive. I didn't know exactly -- I
14 don't know what exactly I was expecting to happen
15 when we notified the manufacturer, but I do
16 believe that -- I believed at the time that it was
17 going to involve a discussion, it was going to
18 involve some technical back-and-forth and perhaps
19 an application of some of the repairs and
20 mitigations that we had developed at the time.

21 That's not what happened. Instead what
22 happened was that we encountered a great deal of
23 resistance, pushback from the manufacturer and an
24 active effort to ask us, as university
25 researchers, to suppress our research and to not

1 publish the fact that there were vulnerabilities
2 in the system.

3 MS. CHARLESWORTH: Excuse me. Was that
4 -- you mentioned it was on a chip.

5 I mean, when you say "manufacturer," is
6 that the chip manufacturer?

7 MR. GREEN: The chip manufacturer.

8 MS. CHARLESWORTH: Okay.

9 MR. GREEN: Yes.

10 MS. CHARLESWORTH: Thank you.

11 MR. GREEN: Yes. So instead of
12 repairing the system and discussing ways to repair
13 the system, the manufacturer spent considerable
14 resources in an effort to prevent us from
15 publishing the work.

16 One of the several levers for that
17 effort was to raise the specter of an expensive
18 legal action based on the anti-circumvention
19 provisions of Section 1201.

20 Since our work in that case did involve,
21 as a small component, some degree of reverse
22 engineering of software and the bypassing of an
23 extraordinarily simple TPM. So in my opinion, the
24 Section 1201 was never intended to prevent
25 security researchers from publishing their

1 results.

2 In the moment though, when you're a
3 penniless grad student and somebody is presenting
4 you with a possibility of a lawsuit you can't
5 possibly afford, it's hard to argue about the
6 merits of a case or the intent of a law. It's
7 more tempting to simply comply and hide a serious
8 vulnerability from public view.

9 MS. CHARLESWORTH: Can I -- I'm sorry. I
10 promised I would interrupt you.

11 MR. GREEN: Sure.

12 MS. CHARLESWORTH: And I'm doing it.

13 MR. GREEN: Go ahead.

14 MS. CHARLESWORTH: But 1201(j) -- now
15 that you have a better understanding of the law,
16 can you explain why you think that might or might
17 not have applied to that scenario you just
18 described?

19 MR. GREEN: Well, so my understanding of
20 the law is that -- and you -- stop me, Blake, if
21 I'm saying anything wrong.

22 There are two issues. There is the
23 bypassing of a technological prevention measure, a
24 TPM -- a protection measure, sorry -- that allows
25 you that -- that protects a copyrighted work. And

1 separately, there is the issue of trafficking in
2 tools that allow people to circumvent.

3 And so both of these issues could
4 potentially be an issue depending on what it means
5 to traffic.

6 In this case my understanding is that
7 the issue was simply bypassing a TPM that may or
8 may not have prevented -- protected a copyrighted
9 work, such as a piece of software. That was what
10 was raised to us at the time.

11 MS. CHARLESWORTH: Okay. But there's an
12 exemption for security testing.

13 Professor Reid, I think, has -- did you
14 want to comment on that on behalf of --

15 MR. REID: Sure. And I hope we can get
16 into this more today. There are actually several
17 exemption sections in Section 1201, including
18 Section 1201(j) for security tests, Section
19 1201(g) for encryption research, and Section
20 1201(f) for reverse engineering.

21 And I'm sure other folks on the panel
22 can speak to these.

23 But as we detailed in our comments,
24 there are shortcomings with each of these -- these
25 exemptions. So for example, Section 1201(j), we -

1 - as we argued, fails to provide the sort of
2 upfront certainty that folks need to know whether
3 their security testing is going to be exempted or
4 not because, for example, it's got a multifactor
5 test that gets looked at after the fact that
6 depends on things like whether the information
7 derived from the security testing was used solely
8 to promote the security of the owner or operator
9 of such computer and whether the information
10 derived from the security testing was used or
11 maintained in a manner that does not facilitate
12 infringement and so on and so forth.

13 And so I think the argument that we
14 would make, if God forbid someone actually did
15 follow through on a threat to sue Professor Green,
16 is we might well argue that Section 1201(j)
17 applies or that Section 1201(g) applies or that
18 Section 1201(f) applies.

19 So I don't want to lay out a blueprint
20 here for how those wouldn't apply because we might
21 have to use them someday.

22 But as we've asked the office to do
23 several times in the past and as the office and
24 the librarian have done, we're asking for some
25 additional clarity to make clear for folks up

1 front before they start a project that, if they're
2 proceeding in good faith, that they're doing the
3 right thing, they're doing this only for security
4 testing or security research and they're not doing
5 it to facilitate any sort of copyright
6 infringement, that they're free and clear.

7 And that's been the basis on which the
8 register granted the exemptions in 2006 and 2010,
9 and we think that -- or we hope the office will
10 provide that direction again this time around.

11 MS. CHARLESWORTH: Right. No. Thank
12 you.

13 And, Professor Green, when were these
14 events -- the story you were telling about the
15 chip? When did that --

16 MR. GREEN: This took place in 2004.

17 MS. CHARLESWORTH: 2004.

18 And I guess, just to put a little finer
19 point -- and I understand what you're saying about
20 the ex-post versus ex-ante analysis, Professor
21 Reid.

22 But do you think that the activities
23 that Dr. Green was describing would -- I mean, in
24 your view, would they fall into the one of the
25 exemptions?

1 MR. REID: I mean, I think it's hard to
2 look at something that happened that long ago. I
3 mean, I don't want to opine without getting into
4 the deep specifics of it.

5 And, again, it's the sort of thing that,
6 if we were in court, I would absolutely argue that
7 they were -- that they were covered. I would
8 argue that there was no copyrighted work. I would
9 argue that there is no copyright infringement. I
10 would argue --

11 MS. CHARLESWORTH: That's a very lawyerly
12 response.

13 MR. REID: But I think if I were
14 advising Professor Green beforehand -- and, again,
15 I'm speaking hypothetically because I wasn't there
16 for all of the details of this -- that he should
17 be nervous about it because a lot of the
18 provisions in this law are ambiguous and we don't
19 ultimately know how they would be applied.

20 So that's the point we're trying to get
21 at is the issue of certainty.

22 MR. GREEN: So I can actually add a
23 little bit --

24 MS. CHARLESWORTH: Sure.

25 MR. GREEN: -- a less hypothetical to

1 that.

2 We were advised at the time by the
3 Electronic Frontier Foundation. The attorneys
4 there provided us with pro bono representation.
5 And we were told that at the time they could
6 provide no guarantee that any of the exception
7 exemptions at the time in the law would have
8 protected us if we were sued under that -- under
9 Section 1201.

10 They didn't say that we were necessarily
11 violating the section. They simply told us that
12 the complexities of those exemptions were such
13 that they could provide no guarantee to us as
14 graduate students.

15 MS. CHARLESWORTH: Okay. And was that -
16 - did you receive that information before you
17 embarked on the testing project or after you got
18 the letter?

19 MR. GREEN: We received that information
20 -- we spoke about it before, during, and after we
21 were -- we were --

22 MS. CHARLESWORTH: So you actually --
23 you sought legal advice before you went down this
24 path?

25 MR. GREEN: Yes. My professor at the

1 time had been through an experience very similar
2 to this and knew to do this beforehand.

3 MS. CHARLESWORTH: And --

4 MR. GREEN: We would not have.

5 MS. CHARLESWORTH: Okay. But you
6 decided to proceed in any -- anyway?

7 MR. GREEN: Yes.

8 MS. CHARLESWORTH: Okay.

9 MR. GREEN: Our view is that it was
10 necessary.

11 MS. CHARLESWORTH: Okay. Go ahead and
12 finish your --

13 MR. GREEN: Sure.

14 MS. CHARLESWORTH: -- statement.

15 MR. GREEN: Okay.

16 MS. CHARLESWORTH: See.

17 MR. GREEN: My statement's almost over
18 anyway.

19 So what I would like to say is that, in
20 that case, we were very fortunate to have
21 representation from the Electronic Frontier
22 Foundation, which gave us the confidence to go
23 forward.

24 And, of course, we were university
25 researchers and grad students. We felt that the

1 probability of a public lawsuit was relatively
2 low. As a result of that, the system has been
3 published -- I'm sorry -- the system has been
4 repaired. We were able to publish our results.

5 But without that, the system may not
6 have been repaired. It may still -- it might
7 still be broken today.

8 So I'm not as naive anymore. While I
9 still conduct research that involves commercial
10 security systems, I now begin every project with a
11 call to a lawyer to evaluate, among other things,
12 whether there's a possible violation of Section
13 1201 and how to mitigate the risk to myself and to
14 my own graduate students.

15 I'm still fortunate to receive pro bono
16 representation from organizations such as the EFF,
17 but many researchers are not so fortunate.

18 Moreover, good-faith research should not
19 require the assistance of lawyers. At a minimum,
20 the need for legal representation significantly
21 increases the cost of each research project. At
22 worst, it works to dissuade the necessary kind of
23 research that we desperately need more of.

24 Thank you.

25 MS. CHARLESWORTH: Thank you, Professor.

1 Professor Reid?

2 MR. REID: Thank you and good morning.

3 I'm going try to keep my statement short
4 so we can get to the many more questions. I know
5 there are a lot of issues outstanding.

6 Just at the outset, I want to thank the
7 office, and to the NTIA, for your continuing
8 consideration of this issue. It's one that's
9 persisted a long time, and it's a really serious
10 one. So we thank you for the extended time in the
11 hearing today.

12 It's actually been just over six years
13 since I first came before the office back in 2009
14 with Professor Alex Halderman. And it's been
15 about a decade since Professor Halderman first
16 appeared before the office with Ed Felten during
17 Sony rootkit saga in the 2006 rulemaking.

18 Back in 2009, we urged you and your
19 former colleagues to grant a broad exemption for
20 Section 1201 for good-faith security research. And
21 Professor Halderman and I warned the office of
22 increasing flaws in TPMs and of Section 1201
23 substantial chilling effects on security
24 researchers that are attempting to study and fix
25 those flaws in good faith.

1 Noting the shortcomings of the built-in
2 statutory exemptions that we just discussed, we
3 predicted that the Sony rootkit, SafeDisc, and
4 SecuROM -- which were some of the problematic TPMs
5 of that time -- would not be the last TPMs to
6 cause collateral security harm. And we urged the
7 office to allow security researchers to react
8 accordingly to evolving threats.

9 The last six years, which are
10 underscored by the substantial record in this
11 proceeding -- and which you'll hear more about
12 from Professor Green and his colleagues today --
13 illustrated that, if anything, we've absolutely
14 underestimated the widespread proliferation of
15 security vulnerabilities that could be both caused
16 by and concealed by TPMs.

17 As we'll discuss today, these
18 vulnerabilities now persist not just in music and
19 video games but in the vast array of software that
20 has become increasingly intermingled with a vast
21 array of everyday consumer goods that comprise the
22 Internet of things, which include cars and medical
23 devices with elaborate but vulnerable networking
24 features and in the software that underpins the
25 Internet and the wide variety of applications that

1 ride atop it.

2 Moreover, the chilling effects that we
3 urged the office to recognize in 2009 have become
4 ever more pernicious. As you heard from Professor
5 Green, a room full of the nation's top security
6 researchers stand before you today, and many more
7 of them have affirmed their views on the record
8 highlighting the threats that they, their
9 colleagues, and their students face in simply
10 trying to make America a safer place to live and
11 to compute.

12 As the office acknowledged in 2010,
13 while Section 1201's built-in exemption
14 underscores Congress's recognition that security
15 is a serious, overriding national priority, those
16 exemptions still don't provide the certainty that
17 researchers need to ensure that their good-faith
18 efforts will not meet with unscrupulous attempts
19 like Professor Green described to silence their
20 work protected by the First Amendment and to
21 protect consumers -- which I know Ms. Moy will
22 speak to -- from serious and often life-
23 threatening flaws in the wide universe of software
24 that exists today.

25 In 2010, Register (ph) Peters rejected

1 Professor Halderman's prediction of worsening
2 security vulnerabilities stemming from TPMs as --
3 and I quote -- "unverifiable, contradictory, or
4 speculative" and recommended against creating a
5 broad exemption.

6 And I think, unfortunately, the
7 intervening five years is replete with evidence
8 that Professor Halderman's prediction was
9 prescient and correct.

10 You now have before you a lengthy record
11 of security vulnerabilities that could have been
12 avoided had security researchers acting in good
13 faith not be chilled by the absence of a workable
14 exemption in Section 1201.

15 I just want to close by saying the
16 researchers who are before you today, including
17 Professor Green, are the good guys. They care
18 about abiding by the law, and they're here because
19 they need you to clear breathing space for them to
20 do the right thing.

21 Without your help, they'll be losing an
22 arms race to bad guys who are, as we speak,
23 circumventing TPMs and exploiting existing
24 vulnerabilities and who don't care about the
25 consequences of violating Section 1201.

1 Today, the office has the opportunity to
2 make the right decision for the next three years
3 by ensuring that security researchers sitting
4 before you today and their colleagues and students
5 who aren't here have the clarity and the certainty
6 that they need to ensure our nation's
7 cybersecurity and protect millions of Americans
8 from serious harm.

9 The record and the law are clear, and so
10 are the consequences for neglecting them. The
11 office should grant -- should recommend and the
12 librarian should grant a clear certain exemption
13 for good-faith security research.

14 Thanks, and we look forward to your
15 questions.

16 MS. SMITH: The exemption that was
17 granted in 2012 was limited to video games, but
18 did you find it a workable exemption for video
19 games?

20 MR. REID: I think the issue with the
21 exemption -- I think it was granted in 2010. My
22 memory may be slipping on that too.

23 The issue was not with the piece of the
24 exemption that was granted for video games but
25 that the vulnerabilities around the DRM that was

1 attached to video games was SecuROM and SafeDisc
2 and several related pieces. That was just one
3 piece of an evolving sort of threat.

4 So previously it had been the rootkit.
5 Then it was SecuROM. But the evolving piece of it
6 ended up being in things like we're going to talk
7 about today, in cars and in medical devices and
8 that sort of thing.

9 So I think it was that narrow piece that
10 said, "Hey, security researchers, if you want to
11 pursue an agenda around -- that involves
12 circumvention, that involves looking at security
13 flaws and technological protection measures, it's
14 okay if it's for video games but it's not okay if
15 it's for anything else."

16 So I think --

17 MS. SMITH: Yes. My question is, for
18 video games specifically, the language included
19 different provisions than what you have proposed
20 on a broader level.

21 So, for example, for video games, it
22 said that the information derived from security
23 testing must be used primarily to promote the
24 security of the owner, operator of the computer,
25 or the information should be used or maintained in

1 a manner that does not facilitate copyright
2 infringement.

3 Those are two limitations that I don't
4 see in your current proposal. And I'm wondering -

5 MR. REID: Sure.

6 MS. SMITH: -- whether or not they
7 restricted research to be performed on video games
8 for what was granted in 2010.

9 MR. REID: I mean, again, it's hard to
10 tell you because the flaws and -- and I'm sorry
11 I'm going to respond with the same answer that I
12 gave to the last question.

13 It was hard to test the exemption
14 because the subsequent vulnerabilities that
15 evolved were not necessarily in video games. And
16 I think what you'll hear from a lot of folks today
17 is they took a look at the exemption and said, "We
18 just got this narrow exemption for video games.
19 We're not going to do research in this area."

20 So I can't tell you how those
21 limitations played out in practice for people
22 because there was so much chill that came from
23 just being able to focus on video games and
24 nothing else that I can't tell you how those
25 limitations worked out.

1 And I think if you asked --

2 MS. SMITH: Okay.

3 MR. REID: -- us to talk about how they
4 would work out if you added them to a broad
5 exemption today, I think we would have some of the
6 same concerns that I -- that I mentioned earlier,
7 which is that they don't have any certainty.
8 They've got words like "primarily."

9 What exactly does that mean? So we saw
10 in the cell phone unlocking context --

11 MS. SMITH: Well, in your proposal, it
12 says "for the purpose." I mean, you can only take
13 it so far, "primarily for the purpose" or "for the
14 purpose."

15 How much more certainty does that
16 provide you? In the statute, you list the
17 exemptions that -- solely for the purpose. So we
18 might want to read a little bit into rational
19 intent.

20 MR. REID: I mean, I guess all I can
21 respond is that the more certainty we can get out
22 of the exemption, the more mileage researchers are
23 going to get out of it. And the language like
24 "primarily" that evokes a post-hoc judgment is
25 going to be problematic because it's going to be

1 hard for counsel to people like Professor Green to
2 say up front, "Well, is what you're doing
3 primarily for this purpose or not so much?"

4 The easier it is to answer that
5 question, the better.

6 MS. CHARLESWORTH: But there's always
7 going to be post-hoc judgment, right?

8 MR. REID: Sure.

9 MS. CHARLESWORTH: I mean, in other
10 words, if you end up in court on something like
11 this, you're always going to have a court looking
12 at whether you fall in the exemption.

13 And I take the point that some of the
14 language here, you know, is -- you know, it's a
15 multifactor test and kind of a balancing test.
16 Maybe there are different ways you could structure
17 a standard that might be more or less predictable.

18 But I think that -- you know, I mean, I
19 would ask the same question. I mean, what is good
20 faith? You know, a court is going to be looking
21 backward at the events if you're litigating this,
22 and they're -- you know, we have to draft language

23 MR. REID: Sure.

24 MS. CHARLESWORTH: -- if we're going to
25 grant an exemption.

1 So and this goes for, I think, everyone
2 here. You know, we're -- we want to understand,
3 again, sort of where you're -- I mean, to Regan's
4 point, you know, we want to understand where
5 you're coming from and what kinds of limitations
6 or -- you know, might be appropriate in language
7 that sort of balance the need for maybe less of a
8 post-hoc analysis or -- and, you know, with kind
9 of some definition of what it is we would be
10 allowing.

11 MR. REID: Sure.

12 MS. CHARLESWORTH: Okay. So that's --
13 that's why it's helpful to explore -- the language
14 and think about, like, looking at -- I mean, we
15 have some -- Congress did act in this area. And so --

16 MR. REID: Sure.

17 MS. CHARLESWORTH: -- that's really good
18 guidance, though, at least about what Congress was
19 thinking at the time. So that -- we're kind of --
20 that's one sort of very important benchmark for
21 us, as we discuss these issues.

22 MR. REID: So, I mean, -- I
23 think I'd underscore to the extent a limitation
24 like the ones that were going to previously winds
25 up in the exemption and we have some concerns

1 about that -- to the extent you can make clear in
2 your guidance in the order about what those
3 limitations mean and what sort of circumstances
4 they cover and which ones they don't -- for
5 example, the limitation about copyright
6 infringement or being used to facilitate copyright
7 infringement.

8 I think we've heard some concerns from
9 the opponent in the record here that simply
10 publishing information about a particular TPM or
11 about particular copyrighted software, that might
12 be facilitating copyright infringement under a
13 really broad theory of what that means.

14 And so I think if you can provide
15 guidance that -- the facts that we're concerned
16 about here -- and we've outlined these -- and we
17 tried to do this in pretty strong detail in our
18 comments, which are investigating security flaws,
19 doing the research into it in a classroom
20 environment for the most part and then being able
21 to publicly disclose in a responsible way the
22 results of that research, that that's what's
23 covered under the exemption.

24 I think if you can provide guidance that
25 enables that, then that's -- that's the most

1 important piece we're looking for out of these
2 limitations.

3 MS. CHARLESWORTH: Okay. I guess I had
4 one more question.

5 MR. REID: Sure.

6 MS. CHARLESWORTH: When you say "a
7 classroom environment" -- so tell me more about
8 that and whether, you know, an exemption should be
9 tied to sort of the academic community in some
10 way.

11 MR. REID: Sure. And I'll probably kick
12 this back over to Professor Green or others on the
13 panel, if you don't mind.

14 But I'll just say at the outset: I
15 think it's important from the context that we're
16 coming from that students are able to work on
17 this. This is a really important piece of
18 Professor Green's work.

19 But I don't think we would support a
20 limitation that would restrict it to classroom
21 use. I think the contributions of folks from the
22 private sector and even from the amateur community
23 of security researchers or folks that are out
24 there building skills at doing this kind of stuff
25 are really important.

1 And I think Professor Green could
2 probably speak to that a little better than me.

3 But I think we would be uncomfortable with a
4 limitation that restricted it to the classroom.

5 MS. CHARLESWORTH: Yeah. I mean, not
6 just the classroom. But should sort of any
7 project of this nature be overseen by a university
8 scholar such as yourself, Dr. Green, or where you
9 could have students working with you?

10 I mean, that's obviously another big
11 factor. Who could -- who could use the exemption
12 and should that be limited?

13 MR. GREEN: I would be -- I would be
14 very concerned about an exemption that focused
15 only on university research. And the reason is
16 that the most dynamic and the most important
17 research being done right now is being done by
18 people in the private sector and people we refer
19 to as commercial security researchers.

20 So, for example, the vehicle security
21 research -- which I'm sure you discussed in the
22 previous hearings -- is being worked on by --
23 funded by DARPA but being worked on by individuals
24 such as Charlie Miller, who's not affiliated with
25 a university. Very similar situation with a great

1 deal of other security research.

2 It would be a huge loss to restrict the
3 exemption to that.

4 MS. CHARLESWORTH: Although a lot of
5 that is authorized by the manufacturers, isn't it?

6 MR. GREEN: Some is authorized, but the
7 vast majority of security research is done by
8 private individuals who have access to open-source
9 software or to devices. There have been cases
10 very recently with security researchers being
11 told, "You found a vulnerability. We have to --
12 you may have to back off because of a possible
13 DMCA violation."

14 Just a couple of weeks ago, that
15 happened. So there's a great deal of research
16 being done without authorization.

17 MS. CHARLESWORTH: Okay. I think we'll
18 -- oh. We'll move to Mr. Sayler.

19 MR. SAYLER: Thank you and good morning.

20 I'd like to start by thanking the
21 members of the Copyright Office and the NTIA for
22 inviting me and my colleagues to testify before
23 you here today.

24 Like it says on the placard, my name is
25 Andy Sayler. I'm a doctoral candidate studying

1 computer science and security and privacy at the
2 University of Colorado in Boulder.

3 I'm joining you today as a member of the
4 Samuelson-Glushko Technology Law and Policy Clinic
5 at Colorado Law and on behalf of our client,
6 Professor Green.

7 As you're aware, we filed several long-
8 form comments on behalf of Professor Green in
9 support of the proposed class 25 exemption
10 allowing the circumvention of TPMs for the purpose
11 of performing good-faith security research.

12 I'd like to reiterate our request that
13 the Copyright Office grant the proposed class 25
14 exemptions for the reasons I'll -- and I'm sure
15 others -- will discuss here today.

16 In particular, this exemption is being
17 considered at a critical time in the history of
18 cybersecurity and research and development.
19 Computers are ubiquitous components of our daily
20 lives from the cell phones in our pockets to the
21 vehicles we drive to life-saving medical devices
22 and much more.

23 Unfortunately, it's rare to have a week
24 go by without a new story about some new security
25 flaw or data breach in our computing systems.

1 Indeed, just last week, Professor Green, Professor
2 Heninger -- who hopefully will join us at some
3 point -- and a number of their colleagues released
4 a report disclosing the logjam vulnerability in
5 the core protocol we use to keep the Web secure.

6 Such research demonstrates the critical
7 importance of independent good-faith security
8 research in the community.

9 Last week's vulnerability is not unique.
10 It joins a list of significant vulnerabilities
11 discovered by independent researchers in a range
12 of software and devices over the previous few
13 years, including the Heartbleed SSL flaw, the
14 Shellshock Bash bug, and numerous vulnerabilities
15 in vehicles and medical devices.

16 MS. CHARLESWORTH: Can I -- I'm sorry.
17 Just on the one you mentioned from a week or so
18 ago, the logjam issue, I mean, was that done
19 without circumvention?

20 MR. SAYLER: I think Professor Green,
21 being the expert on the panel, would be the one to
22 comment on that.

23 MR. GREEN: It involved primarily
24 looking at public specifications, but there was
25 some degree of looking at other devices. I'm not

1 sure if it involved circumvention in that case.

2 MS. CHARLESWORTH: So we don't know.

3 Okay.

4 MR. GREEN: Yeah. Thank you.

5 Continue, Mr. Sayler.

6 MR. SAYLER: Independent security
7 research, much as Professor Green noted, is
8 actually funded by the U.S. government via the
9 National Science Foundation, DARPA, and other
10 agencies. It is a critical component of the
11 effort to better secure the software and computing
12 devices on which we rely.

13 Unfortunately, Section 1201 is being
14 used to discourage the very independent security
15 research that has shown itself to be critically
16 important to our cybersecurity. Congress never
17 intended Section 1201 to be used to suppress good-
18 faith security research and even included the
19 specific exemptions we've mentioned for encryption
20 research and security testing in the original
21 statute.

22 These exemptions, however, are somewhat
23 ambiguous and impose a number of undue burdens on
24 researchers, making it difficult for them to know
25 whether or not their work runs afoul of the law.

1 Furthermore, certain parties with an interest in
2 suppressing public knowledge regarding the flaws
3 and insecurities in their products have taken
4 advantage of the ambiguities in Section 1201 to
5 threaten security researchers performing good-
6 faith research or disclosing the flaws they
7 discover.

8 As Professor Green mentioned, just two
9 weeks ago, a researcher for the security firm
10 IOActive was threatened under Section 1201 for
11 disclosing serious flaws in the CyberLock line the
12 secure door locks. CyberLock secure door locks.

13 These ambiguities and the threats they
14 allow have the net effect of discouraging
15 researchers from studying the security of many of
16 the computing devices on which we rely.

17 Even those who do choose to study such
18 software and devices must do so at significant
19 personal risk of liability and are forced to incur
20 unreasonable legal expenses to mitigate that risk.

21 It is thus imperative that the Copyright
22 Office grant the petition for this exemption,
23 relieving researchers of the undue burden placed
24 on them by Section 1201.

25 For the noninfringing actor practicing

1 good-faith security research, such an exemption is
2 critical to ensuring the security of our nation,
3 the security of its citizens, and the security of
4 the digital world at large.

5 Thank you for your time, and I look
6 forward to your questions.

7 MS. CHARLESWORTH: Okay. Mr. Stanislav?

8 MR. STANISLAV: Put my props up front
9 for you.

10 So good morning. My name is Mark
11 Stanislav. I am a security consultant and
12 researcher.

13 Last year, I assessed the security of an
14 Internet-connected children's toy, which is right
15 here, that allows parents to send audio messages -

16 MS. CHARLESWORTH: I'm going to -- let
17 the record reflect that you're holding up
18 something.

19 What is that?

20 MR. STANISLAV: A plastic -- it's a pig.
21 His name is Snort. Literally, the name of the
22 toy. And it's a mailbox because that -- the audio
23 communication that you can send to your child to
24 this device is effectively a mailbox for the child
25 to get a letter but via audio.

1 MS. CHARLESWORTH: So that would go --
2 forgive me for not being familiar with that.

3 MR. STANISLAV: It's a brave, new world.
4 I understand.

5 MS. CHARLESWORTH: So that would go --
6 like, the child would be near that and would hear
7 -- would hear you transmitting an audio
8 communication?

9 MR. STANISLAV: It will actually "oink"
10 at you to let the child know there is a new
11 message. And then there is a "play" button and
12 then the arrow can actually have the child reply
13 back to the parent or whomever might be sending
14 that message.

15 MS. CHARLESWORTH: So it's like a baby
16 voicemail system?

17 MR. STANISLAV: Yes. That is a great
18 way to put it.

19 MS. CHARLESWORTH: Okay. Thank you. You
20 may continue.

21 MR. STANISLAV: You're welcome.

22 And so, as I mentioned, the child can
23 reply back using this toy.

24 I was able to determine that the
25 security features of this device were flawed,

1 allowing an unauthorized person to be able to
2 communicate with the child's device.

3 Worse, however, was that the same person
4 that would have access to send these messages to a
5 child and receive replies back, another flaw in
6 this device platform actually allowed for the name
7 of the child, their date of birth, and a picture
8 of the child to all be gathered as well.

9 Upon completion of my research, I
10 contacted the vendor to explain these issues.
11 Despite my offer to go into details with their
12 engineers, the vendor would not engage with me.

13 Ultimately, my employer at the time
14 received a call from the legal staff of this
15 vendor stating that I must have hacked their
16 company, as that's the only way I could possess
17 this knowledge or have found these
18 vulnerabilities.

19 After a few tense conversations with our
20 respective legal teams, it was determined that the
21 vendor's perception of my actions was not
22 accurate, and productive dialogue finally
23 occurred. The issues were quietly resolved
24 without notifying customers.

25 Still, the situation did make me fear

1 for my livelihood as the DMCA could have been used
2 against me at any point for the circumvention of
3 the authorization controls even though they were
4 very flawed.

5 MS. SMITH: Can I ask --

6 MR. STANISLAV: Yes.

7 MS. SMITH: Did you discuss the specific
8 exemptions of the DMCA for personal information or
9 1201(j) in that instance?

10 MR. STANISLAV: So the legal staff of my
11 employer at the time took over these
12 conversations. I wasn't privy to the direct
13 conversation.

14 MS. SMITH: But you understood that your
15 employer felt that at least there was a risk that
16 you would not be able to rely on 1201(j) or --

17 MR. STANISLAV: Absolutely. My firm
18 that I worked for at the time had numerous
19 security researchers over the last probably 20
20 years. So they were very privy to the concerns
21 around DMCA and what would have been done for the
22 DMCA.

23 Thank you.

24 With the goal of protecting children,
25 you know, honestly, that was worth the unfortunate

1 risk of a lawsuit.

2 The possibility that a pedophile could
3 anonymously communicate over the Internet to a
4 child while possessing details of that child is
5 certainly a concern and a terrifying reality of
6 the modern age we live in.

7 In another example of research, I found
8 that my own home's web camera that I had been
9 using for quite a while actually had
10 vulnerabilities that could allow a criminal to
11 control full access over the device, including
12 looking at the streaming audio and video of the
13 device that was transmitting from my home.

14 MS. CHARLESWORTH: Okay. And I'll just
15 say again, for the record, that you held up a --
16 that's a camera? A web camera?

17 MR. STANISLAV: Yes.

18 MS. CHARLESWORTH: Okay. What we may do
19 after -- well, we may take a break. Since this is
20 a long panel, we may photograph those and --

21 MR. STANISLAV: Sure.

22 MS. SMITH: -- with your permission,
23 enter them as exhibits for the hearing a little
24 later on. Okay.

25 MR. STANISLAV: Not a problem. Thank

1 you.

2 These issues, obviously, directly risked
3 my privacy and possibly the safety of the other
4 camera owners.

5 I contacted the vendor to alert them to
6 these issues and offered my assistance to see
7 these issues resolved. The final e-mail I
8 received from their CTO, after going from a range
9 of friendly to threatening, ended up wanting to
10 meet with me to understand how I found these
11 issues as I may have come across confidential
12 information, in their eyes, during this process.

13 Despite my prompt replies, the vendor
14 stopped replying to me and eventually these issues
15 were again quietly resolved without notifying
16 customers.

17 Looking to today, the entrepreneurs who
18 made this connected children's toy actually have
19 gone on to win numerous awards, including monetary
20 prizes from organizations such as Cisco. One has
21 to believe that their ability to win such prizes
22 and continue their business would have not been
23 possible had a criminal abused these
24 vulnerabilities and actively put children in
25 harm's way.

1 The vendor of my web camera actually had
2 a change in leadership, and the new leadership
3 there apologized for their predecessor's
4 indifference and lack of communication from the
5 prior experience.

6 These are clear examples of how security
7 research not only prevented harm and violations of
8 privacy but also ensured that businesses could
9 continue their business by fixing critical flaws
10 before it impacted their customers adversely The
11 exemption of security research under the DMCA
12 would remove a large obstacle for doing what we do
13 best, helping people that are unaware they are in
14 harm's way or helping businesses putting customers
15 in harm's way unintentionally.

16 Americans are becoming inundated with
17 devices. They are watching us, tracking us, and
18 ultimately possibly endangering us. We live in a
19 time where literally someone's mobile phone can
20 control the oven in your home and set it to a
21 temperature.

22 We have smart TVs that actually have
23 microphones listening to what we are saying all
24 the time in order to act on certain commands it
25 overhears.

1 Please help widen the collective efforts
2 of security research by -- for the researchers who
3 do stay away from the DMCA for fear of legal
4 action. Our collective safety and privacy depend
5 on it.

6 Thank you very much for your time, and I
7 would be happy to answer any questions you have.

8 MS. CHARLESWORTH: Thank you.

9 MR. CHENEY: May I ask a question?

10 MR. STANISLAV: Sure.

11 MR. CHENEY: Mr. Stanislav, have those
12 vulnerabilities been fixed in these products or in
13 subsequent releases of these production?

14 MR. STANISLAV: Yes, sir.

15 MR. CHENEY: Okay.

16 MS. CHARLESWORTH: Professor Bellovin?

17 MR. BELLOVIN: Thank you for giving me
18 this opportunity to talk.

19 I'm Steven Bellovin, a professor of
20 computer science at Columbia University. Before I
21 joined the faculty there, I spent more than 20
22 years at AT&T Labs research and, before that, Bell
23 Labs to the corporate whatevers.

24 Before I go on to what I was going to
25 say, I wanted to make a comment about academic

1 research versus independent security researchers.

2 Academic security research, at this
3 point, is generally concerned with new classes of
4 vulnerability, not -- you know, if somebody found
5 a well-known flaw such as a buffer overflow -- I
6 won't bother explaining that -- in a product like
7 this, it would not be publishable in a computer
8 science venue. It's just not a new, interesting
9 contribution to knowledge.

10 Whereas, this is what is -- most of the
11 flaws that we see affecting the devices that we
12 all rely on are instances of well-known
13 vulnerabilities. These are very serious. They're
14 very important, practical import but are not the
15 subject of academic research. This is conducted
16 by the independent security researchers, and
17 they're the ones who are actively protecting us
18 from flawed devices.

19 So it's not the sort of thing that a
20 professor would be likely to do or students
21 possibly, except as an exercise. And frankly, I
22 would discourage my students from looking for
23 well-known vulnerabilities because it's not going
24 to get them any academic credit, at least not if
25 they're Ph.D. students.

1 It's not the kind of research
2 that academics do at this point. Twenty years ago
3 it was, but it's not -- we're not here 20 years
4 ago.

5 I actually want to go back in my ancient
6 history where I was in high school a very long
7 time ago and learned a program when that was a
8 very unusual thing. And I wanted to understand
9 how the operating system worked.

10 So I wrote a program called "the
11 disassembler" to go convert the binary code of the
12 operating system back into marginally
13 comprehensible source code and studied it. That's
14 what got me to where I am today, studying that
15 way.

16 You know, that was a program that won an
17 honorable mention in a programming contest -- a
18 student programming contest. Arguably, in many
19 circumstances, it would be illegal today if I
20 wanted to go look at, say, something protected by
21 technical measures such as a smart phone.

22 Four years later, I caught my first
23 hackers while I was still an undergraduate.

24 I teach my students how to analyze and
25 attack programs. More than 20 years ago, I co-

1 authored the first book on firewalls and Internet
2 security. We had a chapter called "The Hackers
3 Workbench" to explain here's how you do attack.
4 You have to know this because this is the way you
5 secure your system.

6 I teach my students how to evaluate
7 things, and I teach that one of the ways to do it
8 is to actually try an attack. That's one of the
9 homework assignments that I give. You have to
10 know how to do this in order to secure a system.
11 It's not the only way, but it's one of the ways.

12 I mentioned this book more than 20 years
13 ago. I would add, by the way, that two years
14 later, in 1996, I found a copy of this book online
15 -- it had been scanned and OCR'd online, on the
16 very new-to-the-world Web. The publisher had
17 never heard of such a thing at the time. It took
18 them a month to figure out how to cope.

19 And this was a book that sold over a
20 hundred thousand copies. So I'm not unmindful of
21 the importance of copyright. I personally
22 profited by it a great deal. But I'm also looking
23 for the proper balance.

24 In that chapter called "The Hackers
25 Workbench," I have a page excerpt from a book from

1 1853 -- no copyright issue involved. The book was
2 called "A Rudimentary Treatise on the Construction
3 of Locks," discussing whether or not it was proper
4 to discuss lock-picking and vulnerabilities. I
5 won't read the whole page, but...

6 "If others differ from the lock maker
7 about the quality, it's open to them to say so,
8 and a discussion truthfully conducted must lead to
9 public advantage. Discussion stimulates
10 curiosity. Nothing but a partial unlimited view
11 of the question could lead to the opinion that
12 harm can result. If there be harm, we much more
13 than counterbalanced by good."

14 Thank you.

15 MS. CHARLESWORTH: Thank you, Professor.

16 Professor Matwyshyn? Did I say that
17 correctly?

18 MS. MATWYSHYN: You did.

19 MS. CHARLESWORTH: Oh, wow.

20 MS. MATWYSHYN: Thank you to the
21 esteemed panel for permitting me to be with you
22 here today to speak about the topics that are at
23 issue in our requested exemption.

24 So I'm here in my capacity representing
25 security researchers, but I'm also here as a legal

1 academic who has studied these issues for over a
2 decade and the question of the litigation threats
3 that arise from Section 1201.

4 And I should say my background is as a
5 corporate attorney. I've helped companies start
6 businesses, create intellectual property, protect
7 intellectual property, and engage with both
8 consumers and attackers of their intellectual
9 property.

10 The questions that we're considering
11 today at root deal with a type of frivolous
12 litigation. They are an attempt to mitigate
13 disclosure and conversation around existing flaws
14 that may impact consumers, the safety of our
15 economy, the safety of our critical
16 infrastructure.

17 And as such the request that we're
18 making of this esteemed panel is to help curb the
19 frivolous litigation that arises as a consequence
20 of Section 1201.

21 MS. CHARLESWORTH: So I have a question.
22 I mean, this is a question that really is for
23 probably the entire panel, pretty much.

24 But on the issue of disclosure, I mean,
25 obviously, what you're suggesting is -- you know,

1 and we heard this earlier -- manufacturers tend to
2 shut down the conversation. They want to shut
3 down the conversation.

4 But isn't there a countervailing
5 interest in at least giving a manufacturer of a
6 deficient product some time to correct it before
7 there's public dissemination of the hack?

8 Which, you know, I understand for
9 sophisticated really bad-hat people that are out
10 there working, that's the argument.

11 But for, say, hacking into something
12 more mundane -- say, a video console or something
13 like that -- a video game console -- I mean, there
14 are probably a lot of people who don't know how to
15 do that who might be educated after reading a
16 disclosure.

17 And so I'd be really interested, since
18 you sort of have the law and the technical piece
19 of this, in hearing your thoughts on how to
20 balance those two interests.

21 MS. MATWYSHYN: So in my experience,
22 there are two types of companies. Some companies
23 are very receptive to receiving this type of
24 information; in fact, they welcome it. There are
25 sophisticated entities, such as Facebook and

1 Google and Tesla who have bug bounty programs
2 where they compensate, in fact, researchers asking
3 them to help with securing their products.

4 And so there's this affirmative
5 solicitation. They have processes in place with a
6 clear reporting mechanism on their websites, for
7 example, and internal identifying personnel to
8 engage with these conversations.

9 The second type of company,
10 unfortunately, has not yet grown into that
11 sophisticated model of vulnerability handling. And
12 so it's this second category of company that does
13 not possess the external hallmarks of
14 sophistication that I mentioned with respect to
15 the first category.

16 These are the companies that react
17 viscerally through overzealous legal means and,
18 unfortunately, threaten security researchers. And
19 so, if I may, the PowerPoint that I shared has a
20 copy of one of the DMCA threats that was received
21 on April 29th of this year. And this --

22 MS. CHARLESWORTH: Okay. So this now --
23 Ms. Smith, this -- okay. Yes. This is Exhibit 10
24 -- Hearing Exhibit 10, for the record, that we're
25 looking at now on the screen, which is a letter

1 from a law firm to Mike.

2 (Whereupon, Hearing Exhibit No. 10 was
3 marked for identification.)

4 MS. MATWYSHYN: Yes. So this is a
5 letter from an attorney at Jones Day to Mike
6 Davis, who is a security researcher at IOActive, a
7 security consultancy, in connection with Mike's
8 repeated attempt, as documented in a "Wired"
9 article to contact CyberLock, a manufacturer of
10 locks used in various financial services and
11 infrastructure applications, as I understood their
12 product from their website.

13 Mike Davis attempted to communicate with
14 them on multiple occasions and discuss with their
15 technical team the vulnerabilities that he
16 discovered, in particular, my understanding is the
17 ability to clone the lock, which is a serious flaw
18 in their product line.

19 The attorney here was, in Mike's
20 recounting -- and on the subsequent slide you have
21 a letter -- an e-mail from their general counsel
22 to be explaining the general counsel's experience
23 with interacting with Jones Day on this matter.

24 The attorney from Jones Day used the
25 DMCA as the sole legal basis for the threat

1 against the security vulnerability disclosure.

2 MS. SMITH: Looking at this letter, the
3 third paragraph says, "When I reached out to
4 discuss this matter with you, you declined to
5 share any information about your activities
6 concerning the products."

7 And I'm wondering -- my reading of it as
8 part of the hearing was that, you know, I wasn't
9 sure exactly what had gone on, but there seems to
10 be CyberLock taking the position that Davis had
11 insufficiently disclosed the vulnerabilities.

12 Did you -- and also I'll note, in your
13 proposal, you have outlined an annex that would
14 require, I think, Mr. Davis to disclose the type
15 of things that Jones Day is saying he failed to
16 do.

17 MS. MATWYSHYN: So my understanding is
18 that those disclosable items were shared or were
19 ready to be shared with the technical team. And
20 so you have in additional slides not only a slide
21 from the general counsel but also a subsequent
22 follow-up e-mail that Mike Davis sent to me
23 explaining a little more in detail the exchange as
24 well as identifying some prior instances where
25 he's been threatened with the DMCA.

1 MS. SMITH: That actually makes me wonder
2 whether, if your proposed exemption were just
3 granted in full, whether that would change the
4 outcome of this case.

5 Because, you know, we can grant an
6 exemption, but if a company is going to engage in
7 frivolous litigation -- and I don't know that this
8 is frivolous -- but if it's going to, we can't
9 change, you know, them from taking that posture.

10 MS. MATWYSHYN: So I believe that it
11 would remedy the situation significantly.

12 On the next slide, which I can advance -
13 - which I forgot, sorry -- here, actually, I'll
14 advance two to the note from IOActive's general
15 counsel. And so in the general counsel's
16 perspective on this incident and on similar
17 instances, the general counsel is seeking a strong
18 basis to be able to defend his company.

19 And he expresses concern that merely
20 getting litigation to the point of discovery can
21 cost -- he quotes the figure of somewhere in
22 excess of \$250,000.

23 And so when we're talking about a small
24 security consultancy or an independent researcher,
25 this transaction cost of purely hiring an attorney

1 and engaging with the legal system is cost-
2 prohibitive.

3 And so that's why having an exemption
4 that provides a nice roadmap would give a one-line
5 statement of reassurance that a security
6 researcher or general counsel could send to a
7 potential plaintiff informing them that the
8 conduct of the researcher has been within the
9 strictures of the law and that no basis exists for
10 litigation.

11 And so that would give comfort to the
12 security research community in a dramatic way.

13 MS. SMITH: And so is it Part B of the
14 proposal mainly that you're thinking would have
15 deterred this incidence from happening if the
16 proposed exemption were in place?

17 MS. MATWYSHYN: Yes. I believe that, if
18 this exemption were in place, it would have been
19 far less likely that the attorney at Jones Day
20 would have felt at liberty to mention the Digital
21 Millennium Copyright Act as a basis for potential
22 litigation.

23 MS. SMITH: And that's because --

24 MS. MATWYSHYN: So provided that
25 CyberLock has in place a reporting channel and

1 that the researcher used the reporting channel and
2 the reasonable vulnerability management practices
3 exist and the researcher disclosed the list of
4 disclosables that we've delineated in our
5 proposal, this would provide a clear roadmap for
6 both sides' relationship to each other in the
7 context of a vulnerability disclosure.

8 MS. SMITH: Okay. So they could -- they
9 could fight over whether the disclosure had, in
10 fact, taken place. But there would be a little
11 bit less areas that are murky, you're saying?

12 MS. MATWYSHYN: There would be a
13 significant improvement in the murkiness, and it
14 would be ultimately a more easily discernible
15 question of fact rather than an interpretive
16 matter for the law.

17 MR. DAMLE: Sorry. I have a question
18 about this.

19 So one of the elements
20 here of -- of this is that the -- that the
21 manufacturer or the company have an internal
22 corporate vulnerability management handling
23 process.

24 How would an independent security
25 researcher be able to verify that?

1 MS. MATWYSHYN: So from the perspective
2 of the researcher, the most important piece of
3 this is the location of a prominently placed
4 reporting channel. These additional requirements
5 are not researcher-centric; they're for assisting
6 a subsequent analysis of a situation, if it were
7 to go awry.

8 But the bottom line is we want
9 researchers to use provided channels of reporting.
10 And so if a provided channel of reporting exists,
11 this directs the researcher to use that channel.
12 And that's the most important element from a
13 researcher's ability to assess whether a company
14 is hostile or receptive to vulnerability
15 reporting.

16 MR. DAMLE: Right. So that -- so it
17 seems to me that you're talking about the front
18 door.

19 MS. MATWYSHYN: I am talking about the
20 front door.

21 MR. DAMLE: But then you've separately
22 said in your proposal -- I'm just trying to
23 understand sort of what the element -- all the
24 elements of your proposal.

25 The one that gave me pause was on No. 3,

1 page 2 of your reply comments, which talks about
2 the creation of an internal corporate
3 vulnerability management handling process.

4 And what the opponents have said is,
5 "Look, for an independent security researcher, how
6 would they even know whether a company has those
7 internal processes in place?"

8 MS. MATWYSHYN: Mm-hmm.

9 MR. DAMLE: So setting aside the front
10 door -- which obviously they could find out about
11 -- how would they know about the internal
12 processes?

13 MS. MATWYSHYN: So from the perspective
14 of the researcher, the important element is the
15 front door.

16 MR. DAMLE: Okay.

17 MS. MATWYSHYN: From the perspective of
18 analysis subsequently for a judge or another
19 finder of fact, the question would be not only
20 whether the front door existed but let's say that
21 the front door existed, the front door was used
22 but the rest of these processes were not in place
23 and the vulnerability disclosure goes awry because
24 the report was lost on the desk of someone in the
25 sales department who did not pass it on.

1 MR. DAMLE: Yes. But -- okay. But then
2 it doesn't do -- that element doesn't do -- it's
3 not very helpful, going to Professor Reid's point,
4 in giving sort of ex-ante comfort if you don't
5 know, well, what are the internal processes going
6 to shake out as.

7 MS. MATWYSHYN: So the first -- yeah. So
8 the first point gives immediate, in-the-moment
9 comfort. The other points give comfort knowing
10 that, if the vulnerability disclosure process goes
11 off the rails --

12 MR. DAMLE: Right.

13 MS. MATWYSHYN: -- not because of the
14 failure to report but because the internal
15 processes weren't in place and the subsequent
16 threat is levied against the researcher, that the
17 researcher has a second-tier ability to defend if
18 the later rounds of the vulnerability disclosure
19 are not successful and result in a threat under
20 the DMCA.

21 MR. DAMLE: I see. Okay. All right.
22 Thank you.

23 MR. BELLOVIN: May I add something here?

24 MR. DAMLE: Yes.

25 MR. BELLOVIN: It's often remarkably

1 hard to find out how to report a vulnerability
2 that you have found. More than once -- and I've
3 been doing security research for almost 30 years.
4 More than once -- and I know people all over the
5 industry.

6 More than once, I've been able to help
7 people who've come to me saying, "Steve, I found a
8 problem in such-and-such. Can you help me report
9 it? There's no way to get in contact with this
10 company."

11 I know people at most of the major
12 companies, the security people. I can generally
13 find a way -- an artificial channel.

14 But think of yourself -- put yourself in
15 the position of someone who has found a flaw and
16 doesn't say "not me." What do you do with it? Do
17 you have any choice but to go public if it's a
18 threat to life and safety if there's no mechanism
19 provided?

20 That alone would be a tremendous
21 benefit.

22 MS. MATWYSHYN: If I may, as a case
23 study of a typical disclosure, Professor Heninger
24 was going to provide this panel with some
25 statistics from a particular vulnerability

1 disclosure that she engaged with. So Professor
2 Heninger attempted to contact 61 companies with
3 respect to an existing vulnerability. Thirteen had
4 some kind of contact information available. For
5 the others, she was forced to guess at what the
6 best point of contact might be.

7 There was a human-generated response
8 from 28 of these companies out of 61. A different
9 13 of the companies said that they had already
10 fixed the problem at some point in time. And six
11 subsequently released security advisories because
12 of the report from Professor Heninger's team. And
13 three of those were after the intervention of ICS-
14 CERT contacting the particular vendor in question
15 to nudge the disclosure and correction process.

16 And so that's out of the 61 companies
17 that she could identify were impacted. So that's
18 one case study.

19 MS. CHARLESWORTH: Right. Although, in
20 that case she, I think -- I guess the suggestion
21 is she did a good-faith attempt that she probably
22 documented -- and clearly did because she has all
23 the results --

24 MS. MATWYSHYN: Yes.

25 MS. CHARLESWORTH: -- to notify all

1 those affected companies.

2 MS. MATWYSHYN: Yes.

3 MS. CHARLESWORTH: And in some cases may
4 have been unsuccessful but in some cases was
5 successful.

6 So, I mean, that's another way to look
7 at that. It's a more objective standard rather
8 than having her know, again, to my colleague's
9 point, what the internal processes of these
10 companies may or may not be in terms of judging
11 how to -- how she should behave.

12 MS. MATWYSHYN: So, again, if I may, the
13 judgment point for the researcher is whether there
14 is a front door for reporting. If there is a
15 front door for reporting the vulnerability, the
16 researcher should use it.

17 MS. CHARLESWORTH: Well, that's one way
18 to judge it. But another way is just that you do
19 your -- you make a good-faith effort to track down
20 the company and do -- and document that. And if
21 you -- you know, in many cases, you probably will
22 find them -- in many cases, they may have a front
23 door. In some cases, they won't but perhaps you
24 could figure out how to contact them and keep a
25 record of that.

1 And in some cases, you might be
2 unsuccessful and you could keep a record of your
3 efforts to attempt that.

4 I'm just saying that's another way to
5 sort of approach this problem.

6 MS. MATWYSHYN: Mm-hmm.

7 MS. CHARLESWORTH: I think in some sense
8 you end up with this -- at the -- largely at the
9 same place, but you're not using a standard that
10 requires you to know something about the internal
11 workings of the company.

12 MS. MATWYSHYN: So I agree. This is
13 certainly one paradigm of contact, and it's the
14 one that most researchers currently use.

15 The challenge happens in the
16 researchers' documentation not being believed by
17 the company who, nevertheless, threatens DMCA
18 litigation. And so the transaction cost of the
19 litigation threat is happening even in instances
20 when there is an internal, thorough documentation
21 of the researchers' reasonable attempts to
22 contact.

23 And so --

24 MS. CHARLESWORTH: Right. But you're
25 not -- you're not going to avoid -- I mean, this

1 gets to -- I mean, some companies are just going
2 to do that, right, because they have money and
3 resources to threaten people even if they -- if
4 they can come up with some basis to, you know, in
5 their heads at least, to do that. So you're not
6 going to avoid that entirely.

7 But we're trying to -- we're struggling
8 with if we were to go down this road and grant an
9 exemption --

10 MS. MATWYSHYN: Mm-hmm.

11 MS. CHARLESWORTH: -- how do we deal
12 with the disclosure issue? And so one of the
13 issues we're having with the ISO standard or
14 whatever -- you know, that kind of model is it's
15 hard for people to know what the internal policies
16 of companies are.

17 MS. MATWYSHYN: So, again, the front
18 door is publicly visible on any website. There
19 either is or is no reporting mechanism on a
20 company's web side.

21 MS. CHARLESWORTH: Right. But -- okay.
22 I guess we've gone back and forth.

23 I think some of the standard, as I
24 understand it, is how they handle things
25 internally.

1 MS. MATWYSHYN: Those are secondary
2 standards. The first cut, from the researcher's
3 perspective, is whether there is a visible, public
4 point of reporting. If that exists, the
5 researcher should use it.

6 If the disclosure goes off the rails at
7 some later point, then those secondary internal
8 processes will be assessed, probably with the
9 assistance of counsel.

10 But having that first prong allows for
11 an independent researcher without the benefit of a
12 legal team to have assurance that this is the
13 appropriate reporting channel, this is where they
14 should report, and if that front door is not
15 findable, not visible, not usable, it gives the
16 researcher assurance that the good-faith effort
17 will have an empirical basis for --

18 MS. CHARLESWORTH: Right. But if they
19 don't have a -- I mean, I don't want to belabor
20 this too much. I want to -- but, I mean, if they
21 don't have a front door, I mean, why shouldn't
22 they try other means to contact the company if
23 they can?

24 In other words -- I mean, this happens
25 all the time in copyright when you're trying to

1 find who owns something and you do research
2 basically and try to make a good-faith effort to
3 figure out who owns something.

4 So in other words, if there's no front
5 door -- I mean, basically, what you're saying is
6 "We here should -- we should have a standard that
7 says everyone has to have a front door or people
8 can disseminate their research" is, I think, sort
9 of where this ends up.

10 And on the other hand, you could have a
11 standard that says, "If they have a front door,
12 use it. But if they don't, do -- you know, use
13 good-faith efforts to try and contact them."

14 You know, there's a more nuanced
15 standard, I think, that could also be considered
16 here. I guess that's -- that's what we're driving
17 at.

18 MS. MATWYSHYN: So the -- the basis for
19 this approach that we proposed is arising, as you
20 mentioned, out of the ISO approach that was a
21 negotiated standard across eight years among many
22 different constituencies.

23 And so that is why we have suggested
24 this --

25 MS. CHARLESWORTH: Yeah. I mean, one of

1 my concerns about that standard is that it's like
2 -- those are big-tech -- for the most part, big,
3 sophisticated tech companies, I think, who
4 negotiated and partake of that standard.

5 But, I mean, this law would apply across
6 the board. And I think you're going to have, I'm
7 guessing, a lot of manufacturers and companies out
8 there who may not participate in that, may not
9 have internal resources to be engaged with that
10 kind of process.

11 And so we have to think of them as well.

12 MS. MATWYSHYN: Mm-hmm. So the notion
13 of designating a copyright contact as the
14 appropriate point of contact also for security
15 vulnerability disclosure as one of those points or
16 have some sort of overlapping approach but
17 designating the correct channel from the
18 perspective of the company the same way that they
19 designate the correct channel for copyright
20 reporting?

21 MS. CHARLESWORTH: Well, that's -- for
22 DMCA, that's a statutory requirement and that's --
23 that Congress thought about for a long time and
24 enacted.

25 MS. MATWYSHYN: Mm-hmm.

1 MS. CHARLESWORTH: So -- but, you know,
2 we're in a slightly different posture here.

3 MS. MATWYSHYN: But if I may follow up
4 on that. I think Congress was contemplating the
5 ability of this kind of information flow when
6 Congress discussed and included Section 1201(i).
7 And so, for example, if we look at the language of
8 Representative Markey, when he was proposing this,
9 he mentioned that the goal was to provide an
10 opportunity for consumers to object to personal
11 data-gathering, to have privacy and data-flow
12 integrity considered.

13 And so these issues of the back-and-
14 forth of information flows was presciently
15 considered by Congress. And so the approach of a
16 designated point of contact, Congress considered
17 them the DMCA as well. And so these two policy
18 considerations that permeate the DMCA are, I
19 believe, consonant and so lend themselves to
20 expansion and clarification in the ways that we've
21 proposed.

22 MS. CHARLESWORTH: Okay. Do you want to
23 wrap up and then we'll go on to Professor Blaze?

24 MS. MATWYSHYN: Sure. I can reserve the
25 remainder of my time for questions.

1 But the issues of DMCA litigation
2 threats have been a concern in the security
3 research community for well over a decade, and
4 there are examples of threats such as the one on
5 the screen that date back over a decade.

6 And so this has been a consistent, long-
7 running, frivolous litigation concern arising out
8 of Section 1201.

9 And with that, we look forward to
10 continuing to address any concerns or questions
11 that you have.

12 MS. CHARLESWORTH: Thank you.

13 Professor Blaze?

14 MR. BLAZE: Okay. So first of all,
15 thank you very much for considering our proposed
16 exemption. And thanks for the opportunity to speak
17 with you today.

18 I'm a professor in the computer science
19 department at the University of Pennsylvania where
20 I study how we build secure systems. A focus of
21 my work is the applications of cryptography, but
22 I'm more broadly concerned with the secure
23 implementation of computing systems.

24 Like my colleague Professor Bellovin,
25 prior to entering academia, I worked for about a

1 dozen years at Bell Laboratories, also as a
2 security researcher, doing much the kind of work
3 that I do today but without students or the
4 troubles of getting funding.

5 The -- much of my work, both before the
6 enactment of DMCA and since, has been concerned
7 with or has stumbled upon vulnerabilities in
8 fielded systems. And some of these fielded
9 systems are traditional Internet-connected
10 systems. Others are not.

11 For example, in 1994, I discovered some
12 fundamental flaws in a U.S. government-proposed
13 encryption standard called the Clipper chip. In
14 2008, I examined a number of electronic voting
15 systems and found -- in 2007-2008, I found flaws
16 in a number of fielded electronic voting systems.

17 And in 2004 and in 2005, I discovered
18 some fundamental weaknesses in various
19 wiretappings systems used by the -- by the
20 government for conducting electronic surveillance.

21 I'd like to talk about two examples
22 where the DMCA has specifically either played a
23 role or not played a role in the -- in the work
24 that I've done, though it's loomed over virtually
25 every bit of nontrivial work that I've done since

1 the legislation has passed.

2 The first thing I'd like to talk about
3 is analogous to the IOActive and CyberLock case in
4 Exhibit 10 that was discussed earlier in this
5 hearing.

6 In 2003, I decided to look at the
7 applications of cryptographic techniques to other
8 types of security. And I looked at mechanical
9 locks and in particular the kind of mechanical
10 locks that we use in offices with a master key
11 that can open all of the doors. These are purely
12 mechanical devices.

13 And I discovered a flaw remarkably
14 similar to the flaws discovered by IOActive that
15 allowed somebody to take an ordinary house key and
16 convert that into the master key that would open
17 all of the locks in the system. And I, you know,
18 discussed how you could use cryptographic
19 techniques to analyze locks and it would lead you
20 to this result fairly straightforwardly.

21 And it was, from my perspective, a
22 fairly, you know, interesting example of --
23 illustrative and educational example of using
24 cryptography. But it also had a real-world impact
25 that it demonstrated that master keyed locks need

1 to have their security reevaluated.

2 Now, this was a purely mechanical system
3 and didn't contain, as a result, any TPMs that
4 would bring the DMCA into consideration. And so
5 when I published my work, I did so without fear of
6 having to defend myself against frivolous DMCA
7 claims because such claims really wouldn't be
8 possible.

9 Nonetheless, the lock industry was
10 unhappy about my criticism of its products even
11 though they claimed that they had known about this
12 vulnerability for several decades and had chosen
13 not to fix it because essentially it would be too
14 expensive and make locks a little less convenient
15 to use and more expensive to manufacture.

16 So I was able to, you know, publish my
17 work. It had its educational value. And we were
18 able to warn the industrial lock community about
19 this flaw without the kinds of concerns that I
20 would have had had these -- the only difference
21 been that these locks were implemented
22 electronically rather than mechanically.

23 So the -- you know, essentially the very
24 same technology that IOActive examined in the
25 CyberLock and had to -- to respond to, you know,

1 what I assume is a frivolous DMCA claim, I was
2 able to do without -- without those fears only
3 because I happened to be looking at this in the
4 purely mechanical realm.

5 A second example of work that I've done
6 that's been chilled by the DMCA: In 2011, I and
7 some graduate students of mine embarked on a study
8 of a communications system called P25 that's used
9 as a digital two-way radio system used by first
10 responders, by the federal government, and by
11 others who are concerned with secure, reliable,
12 two-way radio systems.

13 And I examined the standards for the P25
14 system as well as the broad behavior of a variety
15 of radio products that use them for these two-way
16 radio systems used by first responder and by
17 federal surveillance officers.

18 And we discovered a number of
19 fundamental weaknesses in the published protocols,
20 and we discovered a number of usability failures
21 in the way that these are used. But we also
22 discovered a number of ways in which the protocols
23 could lead to implementation failures.

24 In order to study those implementation
25 failures, we would have had to extract the

1 firmware from some of the radio products, which we
2 had access to -- we bought on the secondary
3 market. We went and bought some on eBay and so
4 on. But we were sufficiently concerned that in
5 order to extract the firmware from these devices,
6 reverse engineer it, and study it, and in
7 particular develop and trade in tools that would
8 allow us to extract the firmware from these
9 products, that there would be no way of doing so
10 without running afoul of the DMCA.

11 And so we left that line of research
12 essentially untouched.

13 Now, it's possible that, if we were --
14 if we had the resources and the time to engage,
15 you know, a large legal effort to denote
16 parameters with which we could work, we'd be able
17 to navigate that. But under the DMCA, as written,
18 we were -- we just decided that this was too risky
19 to proceed with.

20 MS. SMITH: So I'm a little bit
21 wondering why 1201(j) did not apply in that
22 instance. I don't know if you sought legal advice
23 or if you could share what that was.

24 MR. BLAZE: So we did -- so, you know,
25 without getting into too many specifics of, you

1 know, the attorney-client conversations we had,
2 you know, essentially, we -- the conclusion was
3 that we were on extremely treacherous territory
4 primarily because we would have had take some
5 devices, reverse engineer the software, attempt to
6 see if the implementation failures that the
7 standard -- that we anticipated might be present
8 in the standard were there, and effectively build
9 a -- build our own test bed along the way to doing
10 that.

11 We did approach a few of the
12 manufacturers of the -- of the equipment and
13 attempted to engage with them and were ignored or
14 rebuffed at every phase. So we realized that this
15 would be a very hostile relationship if we -- if
16 we proceeded.

17 Now --

18 MS. SMITH: So it sounds -- and you
19 don't have to answer if it's a little too legal.
20 But it sounds like maybe some of the concern might
21 have been the anti-trafficking provision in
22 addition.

23 Do you know if that's --

24 MR. BLAZE: That's right. The anti-
25 trafficking provision would have been particularly

1 problematic because we would have required tools
2 for extracting this.

3 There was a colleague -- another
4 researcher in Australia who had also been
5 examining the same system who had developed tools
6 who expressed some interest in working with us.
7 And we basically, couldn't pursue that
8 relationship because of the trafficking
9 considerations. And we'd want to be able to, you
10 know, publish the work that we've done along these
11 lines.

12 MS. SMITH: On a different topic, I'm
13 wondering if there is sort of a norm in your
14 community -- the academic community of sort of
15 trying -- if you can find the person, disclosing
16 in good faith before publication.

17 MR. BLAZE: Right. So, again,
18 certainly, there are simple cases and there are
19 hard cases. In the simplest case, we find, you
20 know, a particular flaw in a particular product
21 that has a well-defined manufacturer
22 and we're able to go to a
23 point of contact or if we
24 can't go to a point of contact, use informal,
25 asking around who should we call.

1 And sometimes we're able to
2 do that. And obviously, as someone,
3 who is an academic in the security
4 community who wants to work in the
5 public interest I don't want to do
6 harm in -- as a result of my work. And
7 disclosing to the -- to the vendor flaws in their
8 products is certainly an important part of
9 avoiding harm.

10 However, in other cases, even
11 identifying the stakeholders is often not so
12 clear. So one example would be flaws that are
13 found in libraries that are used to build a
14 variety of other products.

15 And we won't always know what
16 all, most, or even some of the dominant
17 stakeholders are there.

18 MS. SMITH: So let's take the example,
19 though, when you do know --

20 MR. BLAZE: Mm-hmm.

21 MS. SMITH: When you do know --

22 MR. BLAZE: Mm-hmm.

23 MS. SMITH: -- does it make sense or is
24 it a norm of responsible security
25 research --

1 MR. BLAZE: Right.

2 MS. SMITH: -- to disclose in advance of
3 publication as opposed to concurrently?

4 MR. BLAZE: Right. So I think
5 it's really a question that has to be
6 answered on a case-by-case basis. I
7 think there is certainly a large class of cases
8 where we have a specific vulnerability that we
9 know is limited to a specific product and we can -
10 we can say, "Okay. If this manufacturer
11 repairs it, then we can mitigate this
12 harm."

13 There are other cases in which it's less
14 clear where the vulnerability is present, and it
15 may be more prudent to warn the public immediately
16 that, you know, the product is fundamentally
17 unsafe.

18 So I'm reluctant to make a
19 categorical statement of what the norm is because
20 there's a range of circumstances at work here.

21 MS. SMITH: Maybe Professor Green?

22 MR. GREEN: So one thing I would like to
23 add to that is, in some cases like the
24 vulnerability last week, you have a case of mass
25 disclosure where you simply can't notify all of

1 the stakeholders at once. And that actually works
2 against you because now you have the issue where,
3 if you notify people, they can leak the
4 information, which causes it to become public
5 before you'd like it to, which actually puts
6 people at risk.

7 So you have to be very selective in
8 choosing to whom you disclose. And that actually
9 is very, very difficult. You can't notify people.
10 You're going to be in a position where the only
11 solution you have is to avoid notifying everybody
12 who's affected.

13 MS. SMITH: Meaning the companies?

14 MR. GREEN: Right. So if you have a
15 situation where, let's say, 200 companies are
16 affected, certainly you could notify some
17 companies. You can go to Google. You could
18 probably go to Apple and you could trust that the
19 information would not leak out.

20 But beyond a certain point -- and I've
21 had this happen -- if you notify everybody, the
22 probability that the information becomes public
23 unexpectedly, before significant remediations can
24 be made, rapidly approaches one. It's something
25 that is almost inevitable if you do a mass

1 disclosure.

2 So you have to find a balance between
3 notifying as many people and protecting as many
4 individuals on the Internet as possible without
5 creating a situation where you have an unintended
6 leak.

7 And I'd like to add that Heartbleed,
8 which we're probably all familiar with, was an
9 unintended leak. Too many people were notified of
10 a mass vulnerability, and it came out two weeks
11 before it was supposed to. And as a result, many
12 systems, including Google and Yahoo were not
13 patched.

14 MS. CHARLESWORTH: So in that situation,
15 I mean, is what you're suggesting that you should
16 only notify selected manufacturers? Or what is
17 your solution to that scenario? I mean, because I
18 thought what we were really talking about was
19 notifying the manufacturer versus just
20 disseminating the information publicly.

21 So what -- what is -- if you could
22 elaborate a little bit on --

23 MR. GREEN: Sure.

24 MS. CHARLESWORTH: -- what you're saying
25 and how you would approach the Heartbleed problem

1 correctly, in your view.

2 MR. GREEN: So I think the simplest
3 answer to that question is there is no single
4 answer that you could write down on paper that
5 would cover every situation.

6 With Heartbleed, the situation was you
7 had a massive vulnerability that affected
8 thousands of separate websites. You could notify
9 Google, and you would have a high probability that
10 the information would be -- would stay secret and
11 that they would fix. And that would protect maybe
12 50 percent of the individual end users on the
13 Internet. You could go to Yahoo, and that would
14 protect 25 percent.

15 And you can see that there are
16 diminishing returns as you go to additional
17 websites. As you go to a small website that has
18 maybe 200 end users, now you are protecting 200
19 people by notifying them. But at the same time,
20 the probability that that small website operator
21 leaks the information is fairly high.

22 And then with a public leak, you could
23 have criminals now exploiting that vulnerability
24 before everybody has a chance to fix it. So there
25 has to be a balance. It has to be customized to

1 every single potential security vulnerability.

2 MR. REID: And I could chime in too. I
3 think the theme that you're hearing consistently
4 here is that this is a very complicated issue
5 that's long been the province and the judgment of
6 security researchers who do this as a profession
7 and as an advocacy. And it's only because of
8 the DMCA, as Professor Blaze alluded, that
9 suddenly this has moved into the realm of
10 copyright law.

11 And I think it's getting pretty far
12 afield of the intent of Congress, in enacting this
13 law, to mediate these type of judgments and the
14 complexities of these judgments, which take a lot
15 of negotiation, as Professor Matwyshyn
16 underscored.

17 There are a lot of negotiations to go
18 into developing this ISO standard. So there's a
19 lot of complexities here, and we would strongly
20 caution the office in being too prescriptive about
21 how this disclosure happens, I think, for two
22 reasons.

23 One, if there's no -- if there wasn't a
24 lock involved and the DMCA wasn't involved, we'd
25 just be talking about fair use. And in that case,

1 it would absolutely be up to the researchers'
2 judgment how to do it and there would be no
3 question about what they did with the disclosure
4 or after the fact, the initial -- whatever copying
5 was necessary to do the research is all we're
6 talking about. And after that, I think the
7 research is -- the researcher is free and clear.

8 And I think it's also important to
9 underscore that, when we're talking about the
10 disclosure of the research, we're talking about
11 First Amendment-protected speech. So you've got
12 some serious limitations on the level of prior
13 restraint that you can apply, and I think there
14 are some serious concerns that I have when we
15 start talking about a really ridged structure that
16 governs when someone is allowed to say something
17 and when they're not, particularly when the policy
18 judgments underlying it are complicated.

19 But even if they weren't, I think there
20 are some serious First Amendment issues that you
21 have to consider before you go too far down this
22 road.

23 MS. CHARLESWORTH: Have you briefed the
24 First Amendment issues to us, I mean, other than
25 mentioning them?

1 MR. REID: No. They're not in our
2 brief, and we'd be happy to provide some
3 supplemental briefing on that if that would be
4 helpful.

5 MS. CHARLESWORTH: We'll let you know.

6 But I mean, here's the thing. I mean,
7 kind of where we're coming around is that, when
8 Congress said, "Well, we'll just consider whether
9 you disclosed it as a factor," I mean, this loose
10 standard, maybe Congress had -- was thinking
11 correctly about that when they put that in there.

12 Because what you're -- what I'm hearing
13 from Dr. Green and others is that -- and what
14 you're saying right here -- is sometimes you
15 should disclose, sometimes not; you have to figure
16 out how to do it. I mean, that's maybe why -- you
17 know, perhaps that is the reason behind the
18 standard that we have today in the law for (j).

19 And why -- I mean, you're kind of making
20 a pretty good argument for that.

21 MR. REID: Well, I think there's two
22 responses to that. One, Congress can't contravene
23 the First Amendment even in enacting the DMCA. So
24 to the extent that you're advocating for a reading
25 of Section 1201(j) that would contravene the First

1 Amendment --

2 MS. CHARLESWORTH: I'm not -- I'm not
3 advocating for that.

4 What Congress said, just to be clear, is
5 that, in looking at whether there's a violation,
6 they're going to consider whether there was a
7 disclosure to the manufacturer. I don't think
8 that contravenes the First Amendment.

9 And what I'm saying is -- what I'm
10 hearing now is that maybe that's not such a bad
11 way to think about this.

12 MR. REID: I think -- the other thing
13 that I would put out there is that the factors
14 that are mentioned by Congress in Section (j), to
15 the extent that they're compatible with the First
16 Amendment, can be read as being probative of the
17 intent of the researcher and whether what they
18 were up to was, in fact, security testing or
19 whether it was something else.

20 So you might look to those things as
21 evidence of the act that the security researcher
22 would engage in. But I think reading them as
23 limitations on speech that can be made after the
24 circumvention is performed is constitutionally
25 troubling

1 MS. CHARLESWORTH: Well, that -- that's
2 -- I mean, first of all, that's a brand-new
3 argument that wasn't, as you just acknowledged,
4 briefed before. And I don't read what's in --
5 currently in 1201(j) as constitutionally troubling
6 in the way that you're suggesting.

7 But there's a lot of commentary, and
8 this request for an exemption has to do with
9 disclosure. We've had one suggestion that we
10 basically adopt ISO standards. Some of have
11 suggested that we look at -- to the -- Google as a
12 90-day disclosure standard. You're saying there
13 should be no standard, I think, if I'm hearing you
14 correctly. Although there's one -- you know,
15 Congress clearly had something in mind to some
16 degree at least about whether you fall under the
17 exemption.

18 So that's -- you know, that's what we're
19 exploring.

20 But, I mean, I -- I don't know that -- I
21 mean, Congress clearly had some concern about this
22 area, and many of the commentators have concerns
23 about it as well. And there's a lot of practices
24 around this area.

25 So anyway, thank you for your comments.

1 MR. BLAZE: If I might just respond to
2 the --

3 MS. CHARLESWORTH: Dr. Blaze, yes.

4 MR. BLAZE: -- disclosure issue. I'm
5 sorry. My attorney wants to do that.

6 All right. So one -- as
7 academics and as members of the public research
8 community and as scientists, right, I mean, the
9 aim of our work is to disclose it. Right? I
10 mean, the scientific method demands disclosure.

11 I think there's no question
12 that somebody building -- building tools
13 for the purpose of infringing copyright
14 is not the aim of research.

15 My aim as a researcher is to
16 discover new things and tell everyone and to
17 one, the public. And included in that is,
18 of course, disclosure to the vendor.

19 So I think the question of disclosure,
20 as discussed in the DMCA, is whether or not the
21 work is kept secret or disclosed to the -- to the
22 vendor, not a question of whether it's disclosed
23 to the vendor in advance or what the period of
24 time is.

25 And I think nobody here is advocating

1 conducting -- conducting research and keeping it
2 secret. In fact, quite the contrary. We're
3 trying to protect our ability to do research that
4 we will -- that we will publish and we will
5 disclose and that we can all benefit from.

6 So, sorry...

7 MS. CHARLESWORTH: Okay. Did you -- was
8 that the conclusion of your opening -- so-called
9 opening remarks?

10 MR. BLAZE: I will --

11 MS. CHARLESWORTH: I realize we're past
12 the opening, but that's okay. This is the way
13 this goes.

14 MR. BLAZE: I will shut up now, yes.

15 MS. CHARLESWORTH: No, no, no. That's
16 fine.

17 Dr. Bellovin?

18 MR. BELLOVIN: Yeah. Twice in my
19 career, I have withheld from publication
20 significant security flaws; once in a 1991 paper
21 of mine, once the very last change that we made to
22 the firewalls before sending it off the printer
23 was to delete a paragraph describing an attack
24 that we didn't know how to fix.

25 In both cases, the security community

1 knew about both. The first vulnerability I shared
2 with CERT, the Computer Emergency Response Team
3 funded by the Department of Defense; meetings in
4 Washington and so on.

5 Both cases, because the security
6 community publicly was not made aware of this, the
7 bad guys exploited the flaws before fixes were in
8 place. It was never seen as urgent enough.

9 And the 1990 paper of mine with the
10 flaw, I published in 1995 with some -- almost
11 unchanged except for a couple of paragraphs of
12 commentary saying, you know, "Here's how I
13 discovered it. Here's the history." And we
14 decided to publish after -- first of all, it was
15 being used in the wild by bad guys. And second,
16 my original memo, shared only very closely with
17 very responsible parties, ended up on a convicted
18 hacker's site.

19 So there's no doubt about how the hacker
20 had learned of it. The security community as a
21 whole, though, didn't take it seriously enough
22 because it didn't seem to be a real threat because
23 it wasn't public.

24 In the other case, the vendors were
25 aware of the problem, didn't see a fix. But once

1 it came out in the wild, the security community as
2 a whole -- many more people than I could
3 personally engage -- found solutions, and it's not
4 the threat to the Internet that it seemed to be in
5 1994 because a lot more people were looking at it
6 than found the fix.

7 So in both of those cases, I would say
8 that trying this very private disclosure and not
9 saying anything publicly actually hurt security.
10 We saw the exploits before the community bothered
11 to react or, in one case, was able to.

12 MS. CHARLESWORTH: Professor Matwyshyn?

13 MS. MATWYSHYN: Just four brief points,
14 if I may.

15 So first, to clarify, the security
16 researchers believe that our request stems from
17 primarily 1201(i) and, therefore, the concerns
18 that were noted in the context of 1201(j) are a
19 slightly different set of issues for us.

20 Secondly, on the point of the First
21 Amendment, in our filings, we did reference a
22 First Amendment argument. And there's a footnote
23 to an article extensively discussing the First
24 Amendment implications of security vulnerability
25 disclosure.

1 Should the panel wish to review, I'd be
2 happy to provide a full copy of that document that
3 was referenced in our filings.

4 Next, on the point of Google's period of
5 90-day disclosure, I would like to point out that
6 Google is a member of the Internet Association,
7 which has filed comments in support of our
8 exemptions. So Google is on board with our
9 approach to this problem.

10 And finally, on the point of frivolous
11 litigation, the benefits of an exemption such as
12 ours which provides clarity and comfort to
13 researchers allows for them to feel more
14 comfortable contacting vendors on an earlier basis
15 rather than needing to weigh the risk of
16 litigation to themselves and putting them in a
17 position to decide how to -- what degree of legal
18 risk to separate, which nudge them toward a later
19 contacting of the vendor, to try to give the
20 vendor less time to sue before the public
21 disclosure.

22 And I think Professor Blaze can speak to
23 his experiences of needing to run that calculus
24 for self-preservation concerns on the point of
25 vendor disclosure and litigation.

1 So providing the comfort of the
2 exemption that we're requesting will encourage
3 researchers to contact companies earlier.

4 MS. CHARLESWORTH: Okay. I think,
5 unless -- I think we're going to skip over you for
6 now, Professor Blaze. I don't know if you have
7 anything to add.

8 I felt like -- I felt like you spoke to
9 that issue earlier, but there will be more
10 opportunity.

11 And we'll move over to the very patient
12 other side of the room.

13 Ms. Moy, could you let us know what's on
14 your mind?

15 MS. MOY: Great. Thank you. Thanks so
16 much. And thank you very much for your attention
17 to this issue. Thank you very much for inviting
18 me -- or allowing me, I should say, to testify on
19 behalf of the proposed exemption.

20 So I -- in addition to working on
21 copyright issues, I work a lot on consumer privacy
22 issues. Most recently, I've been doing a lot of
23 work on -- in response to legislative proposals on
24 breach notification and data security standards.

25 So I appear before you today to talk a

1 little bit about consumer privacy concerns in the
2 context of the proposed exemption, some of which I
3 did -- I did comment about in this -- in the -- in
4 this docket.

5 And I think it -- I think it's --
6 although I have -- I have encouraged the Copyright
7 Office to focus most heavily on the strict
8 copyright issues and to -- and to, you know, sort
9 of not weigh the policy issues as heavily as some
10 opponents in particular have suggested that we do.

11 If the context of this rulemaking, I do
12 think that consumer privacy is relevant here for
13 at least two reasons. One is that the statutory
14 exemption for privacy indicates that Congress was
15 concerned with privacy and how 1201 might affect
16 consumer privacy issues.

17 And the other is that some opposition
18 commenters, in the context of this proceeding,
19 have cited consumer privacy concerns as a reason
20 actually to deny the granting of an exemption for
21 security research.

22 So I want to make three -- at least
23 three reasons -- point out at least three reasons
24 that we think it's absolutely critical to
25 encourage the discovery of security

1 vulnerabilities by removing roadblocks such as the
2 anti-circumvention provisions as faced by security
3 researchers who might find vulnerabilities in the
4 consumer privacy context.

5 So first and most obviously, as many
6 others have pointed out, vulnerabilities have to
7 be discovered so that they can be fixed. And
8 vulnerabilities are often what are exposing
9 consumer information.

10 So in this proceeding, expert after
11 expert have emphasized that malicious attackers
12 are not waiting for the good guys to expose
13 vulnerabilities through research so that they can
14 pounce on them for ill ends. Malicious attackers
15 are conducting their own security research, racing
16 to find the exploitable vulnerabilities themselves
17 first. And they're succeeding.

18 So this time last year, "CNN Money"
19 reported that, in the preceding 12 months, hackers
20 had exposed the personal information of roughly
21 110 million Americans. And that's half of
22 American adults.

23 These are just the breaches that we know
24 about. Many entities that suffer breaches never
25 know.

1 So we have to assist the researchers in
2 finding vulnerabilities as soon as possible, most
3 ideally before they're discovered and exploited by
4 malicious attackers.

5 To protect consumers, we have to
6 dismantle the roadblocks, such as anti-
7 circumvention provisions.

8 Second, vulnerabilities should disclosed
9 so that consumers who are considering which
10 products and services to purchase or patronize can
11 incorporate security considerations into their
12 decision-making.

13 Customers have a right to as much
14 information we can provide them as possible about
15 the security features of products that are
16 available in the marketplace. Not only does
17 robust security research, including disclosure of
18 the results, help consumers make informed choices,
19 but it also bolsters vendors' economic incentive
20 to invest in security. And that's because vendors
21 suffer costs associated with reputational harm
22 following a vulnerability or breach made public.
23 And that's as it should be.

24 The cost -- the threat of costly bad
25 press over security failures encourages vendors to

1 do better. We think that that's really important.

2 So, you know, others have spoken about
3 the CyberLock vulnerability. Certainly, if you're
4 a consumer in the marketplace considering
5 different options for a secure lock, as a
6 consumer, you ought to know that there is a --
7 that there is a known vulnerability with the
8 product before you purchase it.

9 Third, vulnerability -- and I think that
10 this one is one that's often overlooked in this
11 context. Vulnerability should be disclosed so
12 that regulators who are enforcing security
13 requirements, unfair trade practices know whether
14 the vendors are adequately protecting personal
15 information as well as whether -- excuse me --
16 whether vendors are adhering to the promises
17 they've made to consumers regarding security.

18 So vendors don't just have a
19 responsibility to consumers to make their products
20 secure and to protect personal information. They
21 also have security responsibilities under the law.

22 For example, the Federal Trade
23 Commission has determined that failing to
24 implement reasonable security standards --
25 reasonable security practices with respect to

1 personal information in many cases constitutes an
2 enforceable violation of Section 5 of the Federal
3 Trade Commission Act. And the laws of many states
4 also require vendors to keep personal information
5 secure.

6 To enforce security standards,
7 regulators need to know how vendors are performing
8 in terms of security. Regulators have some of
9 their own staff who can assist with security
10 research and security audits, but they also do
11 rely in part -- sometimes in large part -- on the
12 work of independent researchers who help them know
13 when vendors are failing on the security front.

14 So just as an example, last year, the
15 FTC brought at least two cases -- one against
16 Snapchat and one against Fandango -- for failing
17 to implement reasonable security practices. And
18 in both of those two -- both of those cases, one
19 of the -- one of the points that the FTC cited in
20 its complaint was that an independent researcher
21 had informed the responsible company of a security
22 vulnerability and that the company had failed to
23 address it.

24 So not only does the FTC use the reports
25 of security researchers to help understand how

1 well companies are doing, it actually -- it
2 encourages companies to develop a process for
3 receiving and addressing reports from researchers
4 regarding vulnerabilities as part of best
5 practices on data security.

6 So just to make that crystal clear, the
7 most prominent federal enforcer of data security
8 recognizes that security researchers play a
9 critical role in improving security.

10 So thank you again for the opportunity
11 to speak here today this issue, and I look forward
12 to any questions you might have.

13 MS. CHARLESWORTH: Thank you, Ms. Moy.

14 Mr. Stallman?

15 MR. STALLMAN: Thank you. I'm Erik
16 Stallman from the Center For Democracy and
17 Technology, and I want to thank the office very
18 much for allowing me to testify today in support
19 of the class 25 exemption.

20 In view of the substantial testimony
21 that's preceded me, I will just make a few points,
22 one that I think is directly in response to some
23 questions that you have been raising and one that
24 underscores a point raised by the panelists.

25 And the first one just has to do with

1 the sufficiency of 1201(j) for security testing. I
2 think there are two reasons why that provision is
3 insufficient. And first is the limitation to
4 security testing that's done only with the
5 authorization of the owner or operator of the
6 computer, computer network, or system.

7 In a world of Internet-enabled devices
8 and services that have software and firmware that
9 might be licensed from any number of parties, it
10 can often be very, very difficult to determine who
11 the appropriate person to seek authorization from
12 is.

13 MR. DAMLE: So I have a question about
14 this because this is -- I've been struggling with
15 this a little bit because it doesn't say -- it
16 doesn't say "the owner of the software." It says
17 "the owner of the computer."

18 And so the sort of prototypical example
19 that one thinks of 1201(j) applying is: I'm a
20 bank. I buy a bunch of servers that run Linux or
21 Microsoft Windows or whatever. And I want to hire
22 someone to come -- a white hat to come and test my
23 security, but I own the computer; I own the
24 computer network.

25 The fact that I don't -- may or may not

1 own the software that's running on that server or
2 on the router -- the Cisco router that I've bought
3 doesn't seem to matter because it says it's the
4 owner of the computer or computer network.

5 MR. STALLMAN: Right.

6 MR. DAMLE: So I'm just sort of curious
7 about that disconnect. So to take an example, if
8 I own a cell phone, you know, I could say I own
9 the computer that sort of constitutes the smart
10 phone.

11 Why isn't sort of that the better
12 reading of 1201(j)?

13 MR. STALLMAN: Well, because I think
14 that it's unclear, like -- is it sufficient to
15 identify one owner or one operator? I mean, you
16 can have a system -- if your banking network is
17 connected to a VPN and that VPN is managed by
18 somebody else and the person who manages the VPN
19 is the person who has introduced the vulnerability
20 into your system, is the owner or the operator of
21 the VPN the person at the bank? Is it the person
22 at the -- whoever operates your ISP? Is it the
23 person who provided -- I mean, I take your point
24 that it's not necessarily the person who owns the
25 software.

1 But particularly with connected devices
2 you can have one -- more than one person as the
3 owner or the operator. And it's unclear whether
4 the statute requires -- and this isn't the
5 definition of the factors -- need to identify one
6 or all potential owners and operators.

7 MR. DAMLE: So I'm just trying to
8 imagine a scenario -- I mean, so the VPN example
9 is one where presumably, if I'm a company and I've
10 hired someone to be a VPN provider for me, I can
11 presumably go to them and say, "Look, I'm
12 concerned about the security. Give me
13 authorization to have someone come in and test the
14 security."

15 So I'm just trying to imagine scenarios
16 where -- because there's just a -- there are a
17 handful of different -- there are a bunch of
18 different types of examples. Take the medical
19 device example.

20 A security researcher could buy a
21 medical device, presumably. And presumably,
22 that's generally what happens is that they buy the
23 pacemaker themselves and then, on that pacemaker
24 that they own, they're running tests against it.

25 MR. STALLMAN: Mm-hmm.

1 MR. DAMLE: And so I think a fair
2 reading of 1201(j) would be that they're the owner
3 of that pacemaker -- that particular pacemaker
4 that they're testing on.

5 MR. STALLMAN: Mm-hmm.

6 MR. DAMLE: And then -- so assume with
7 me that that -- so that's -- assume with me that
8 that's the correct reading of 1201(j).

9 So what are the -- what are other
10 examples of where -- of sort of legitimate good-
11 faith security research that would kind of fall
12 outside of that where you're not necessarily the
13 owner of the computer.

14 MR. STALLMAN: So I'm trying to figure
15 out your example.

16 MR. DAMLE: Right.

17 MR. STALLMAN: So in that case, it's the
18 security researcher, the person who --

19 MR. DAMLE: If you purchase something --

20 MR. STALLMAN: Right.

21 MR. DAMLE: The security researcher
22 purchases a car or a cell phone or a pacemaker --

23 MR. STALLMAN: Right.

24 MR. DAMLE: I don't know. I mean, I
25 don't -- I think it's at least a reasonable

1 reading of 1201(j) -- that language in 1201(j)

2 that you're talking about that they are then the

3 owner of the computer.

4 MR. STALLMAN: And, therefore, have the
5 ability to disclose that vulnerability not just to
6 themselves but to everyone else who might have
7 that computer?

8 MR. DAMLE: Well, I don't know. That's
9 a separate issue. The question is how they -- do
10 they fall within the -- so they don't need -- they
11 get the authorization themselves because they are
12 the owner of the computer, right?

13 So I'm just --

14 MR. STALLMAN: Right.

15 MR. DAMLE: That element of --

16 MR. STALLMAN: Right. I mean, you're
17 asking me to assume that that's a fair reading?

18 It is a reading. I think part of the
19 problem with 1201(j) is that it hasn't been tested
20 that much in litigation. And I think there are a
21 lot of circumstances in which the security
22 researcher would have to rely -- and this is back
23 to my VPN example -- on the bank being, you know,
24 a faithful custodian of their authorization when
25 they go seek it up the chain.

1 And so I think there's a problem with
2 the definition putting you potentially in the
3 position of having to depend on the person from
4 whom you seek authorization, also like seeking
5 authorization from someone else and then you
6 staying all the way down the chain within the
7 scope of that authorization. Because the moment
8 that you fall outside of it, you fall outside of
9 the exemption.

10 MR. DAMLE: Right. And so a related
11 question is: Is the intent of this to allow
12 someone without the authorization of a third party
13 -- so I'm a security researcher, and I want to
14 test HSBC's systems -- pick another bank.

15 MR. STALLMAN: Mm-hmm.

16 MR. DAMLE: So I want to be able to test
17 their systems to know whether they're secure.

18 MR. STALLMAN: Mm-hmm.

19 MR. DAMLE: Is the point of this
20 exemption to allow that sort of activity without
21 the authorization of someone else, some other
22 third party that owns a server that I'm trying to
23 sort of test the security of?

24 MR. STALLMAN: I mean, I think that that
25 may be one point. But I think that the larger

1 point is to have -- is a circumstance where you
2 have something like Heartbleed, something like --
3 where a ubiquitous exploit that is on many systems
4 where you don't have to go around and figure out
5 exactly whose authorization you need to seek
6 before performing that research.

7 And it's also, I think, to help the
8 situation of what is referred to at times as the
9 "accidental researcher."

10 I mean, if someone just comes across a
11 vulnerability while they're -- while they're
12 engaged in wholly separate research, you know, the
13 problem -- they have no -- I mean, they're
14 basically out of 1201(j) because they found that
15 vulnerability before seeking authorization because
16 they didn't know exactly what they were looking
17 for.

18 I mean, part of the issue with a
19 sufficiently robust security research exemption is
20 that often researchers won't know precisely what
21 they're looking for until they start looking. And
22 if they have to stay within the confines of
23 authorization the whole time they're searching,
24 they may not be able to ask the questions they
25 need to ask.

1 MR. DAMLE: So just to ask my question
2 again: So the scenario that I'm positing where,
3 you know, I'm a security researcher and I just
4 want to test this -- the security of a -- take a
5 website at random or take a computer network
6 connected to the Internet at random.

7 Can I -- under your sort of proposal,
8 would I be allowed to do that?

9 MR. STALLMAN: Well, I mean, I think it
10 would depend why you're doing it.

11 MR. DAMLE: Right.

12 MR. STALLMAN: I mean --

13 MR. DAMLE: But let's say I'm -- let's
14 say I say I'm like -- I bank at this bank or I
15 know people that bank at this bank and I want to
16 test that their networks are secure.

17 MR. STALLMAN: Right.

18 MR. DAMLE: Am I able to do that and
19 fall within the proposed exemption?

20 MR. STALLMAN: I mean, I think that so
21 long as your purpose was good-faith security
22 research, yes. I think that if you're just sort of
23 idly curious if the -- if the system is vulnerable
24 --

25 MR. DAMLE: Right. Sure. Sure.

1 MR. STALLMAN: -- I think that's a
2 different story.

3 MR. DAMLE: Okay. But so as long as I
4 have good faith, I don't need the authorization of
5 some third party operator of a website or a system
6 of some sort; I can just go in and test it myself
7 as long as I -- as long as I'm acting in good
8 faith?

9 I'm just trying to understand the sort
10 of metes and bounds of the proposal.

11 MR. STALLMAN: Yeah. So you're entitled
12 to perform research without running afoul of the
13 DMCA circumvention provision -- should not hinge
14 entirely on your seeking authorization. That's, I
15 think, the point of --

16 MR. DAMLE: Okay.

17 MR. STALLMAN: -- of the exception.

18 MR. DAMLE: Okay. Great.

19 MR. STALLMAN: So to move on to the
20 other issue 1201(j) --

21 MS. SMITH: You know what? Can I just -
22 -

23 MR. STALLMAN: Sure. Go ahead.

24 MS. SMITH: -- follow up on that?

25 MR. STALLMAN: Yeah. Uh-huh.

1 MS. SMITH: And I think Mr. Troncoso may
2 want to speak to it to in return to him.

3 MR. STALLMAN: Okay.

4 MS. SMITH: In the BSA's paper, they
5 point out that the legislative history says that
6 the scope of permissible security testing under
7 the act should be the same as the permissible
8 testing of a simple door lock.

9 MR. STALLMAN: Right.

10 MS. SMITH: What the person may not do
11 is test the lock once it has been installed on
12 someone else's door without the consent of the
13 person whose property is protected by the lock.

14 And it seems like --

15 MR. STALLMAN: Right.

16 MS. SMITH: -- when you were talking
17 with Mr. Damle, you were saying, under your
18 proposal, there would be no authorization needed
19 to be requested whatsoever.

20 Is there any way, if we were going to,
21 you know, perhaps modify the current exemption but
22 not allow -- you know, retain some sort of, you
23 know, good-faith effort to get authorization in
24 it, that we could structure that language?

25 MR. STALLMAN: So would it require you

1 to seek authorization before beginning the
2 research? Is that what you're saying?

3 MS. SMITH: Yeah. I'm asking whether
4 you can conceive of any exemption that might be
5 more workable for the security research community
6 that would preserve some sort of an authorization
7 element.

8 MR. STALLMAN: I mean, I go back with
9 the problem of authorization is that it is hard
10 for the researcher to know beforehand exactly what
11 they're looking for and to stay within its scope.

12 And then you have the problem of if they
13 find something, that that authorization can be
14 revoked or can be cabined. And so I think that's
15 -- I mean, I understand you wanting to find some
16 variation of 1201(j) that works, but I think
17 definitionally, if security testing is defined as
18 something that's done only with the authorization
19 of the owner or the operator of the system or
20 computer or network, that you're going to run into
21 situations where there is needed good-faith
22 security research that's not being done.

23 MS. SMITH: Right. I think the concern
24 is that we want to stay within the confines of
25 what the congressional, you know, intent was at

1 the time or at least take that as good guidance.

2 MR. STALLMAN: Mm-hmm.

3 MS. SMITH: And so in Mr. Damle's
4 example, couldn't you just ask HSBC if you were
5 going to do research?

6 MR. STALLMAN: Well, I mean, you could.
7 But what do you do about the instance where you
8 ask and they say no?

9 MS. CHARLESWORTH: You'd be out of luck,
10 I guess.

11 I mean, I guess, to put a sharper point
12 on it, how do you reconcile what you're proposing
13 with the legislative history that Ms. Smith just
14 reviewed?

15 MR. STALLMAN: Well, I mean --

16 MS. CHARLESWORTH: And are you asking
17 the Copyright Office to basically, you know, step
18 away from that?

19 MR. STALLMAN: Well, one, I think that
20 the environment that we live in now and the
21 environment that we lived in when 1201(j) was
22 enacted are different now.

23 And I think that the -- that overall in
24 the legislative history that -- I mean, in the --
25 the House report, they said that the -- and this

1 was where they were talking about the encryption
2 research -- but that the goal of Section 1201
3 would be poorly served if these provisions have
4 the undesirable consequence of chilling legitimate
5 research activities in the areas of encryption.

6 And I think -- I mean, I understand that
7 this analogy was made to the door lock. I think
8 it's a very interesting analogy to apply to
9 digital locks that can be applied and put on many
10 different devices.

11 But I think that the overarching goal of
12 the -- of Congress in providing these exemptions
13 was to make sure that legitimate research
14 activities could continue. And I think that the
15 problem that we're running into now is when people
16 are trying to conduct that research, that 1201(j)
17 is not providing the same scope of protection that
18 they -- that they would seek and, more
19 importantly, that their institutions would seek
20 and that their funders would seek and the people
21 who would publish their research would seek.

22 And so you're seeing a general chilling
23 effect with that uncertainty.

24 MR. DAMLE: So could I ask you
25 something? There's mention -- so there's mention

1 in the papers of things like nuclear power plants
2 and mass transit systems.

3 Are you suggesting that the exemption
4 should allow sort of testing of, you know, live
5 systems that are running nuclear power plants and
6 mass transit systems?

7 I'm just wondering how that kind of
8 research -- maybe that's a question sort of for
9 this side of the table of how that research would
10 be conducted.

11 MR. STALLMAN: Yeah. I mean, I'll defer
12 to that side of the table a little bit, but I will
13 say that many of those systems that we think of as
14 critical infrastructure oftentimes depend on the
15 same type of security that's running applications
16 and services that we think of as noncritical
17 infrastructure.

18 So I would hate to have a situation
19 where you have essentially the stewards of
20 critical infrastructure being able to say, like,
21 kings ex on research that affects not only their
22 systems but systems that, you know, are in widely
23 used customer products and applications.

24 MR. DAMLE: Right.

25 MR. STALLMAN: And by the same token, I

1 would hate to have a -- the ability of a person
2 who uses just the -- you know, the weird pig
3 voicemail thing say that this depends on the same
4 system that runs your mass transit systems so,
5 therefore, you can't conduct this research.

6 MR. DAMLE: Yeah. Although that's sort
7 of my point, which is to say, if this can be
8 tested -- if this can be tested by sort of off-
9 the-shelf software, if off-the-shelf software or
10 things that are purchasable, say, are what run
11 these other critical systems, then you can
12 purchase that other stuff, do the testing on that,
13 and not allow -- not -- I mean, not have an
14 exemption that allows you to test on sort of the
15 live systems that are running a nuclear power
16 plant or keeping an airplane in the air or running
17 our mass transit systems.

18 MR. STALLMAN: Right.

19 MR. DAMLE: I mean, that's sort of the
20 concern is that, you know, if you -- if you allow
21 sort of the testing of live systems, then that's -
22 - that may not be necessary is what I'm
23 suggesting.

24 MR. STALLMAN: Right.

25 MR. DAMLE: And so that's -- that's sort

1 of -- maybe that's the question for the kind of
2 the researchers.

3 Maybe Mr. Reid and then Mr. Bellovin. Do
4 you have thoughts about that point?

5 MR. REID: Yeah. I wanted to chime in
6 and say to the extent that the office takes that
7 reading of (j) that you proposed, the very broad
8 reading, to the point about alleviating chilling
9 effects and reducing frivolous litigation, if you
10 could put that in the record or include that as
11 part of the conclusions in this proceeding, that
12 would be incredibly helpful and we would be deeply
13 appreciative if the office actually takes a
14 position that (j) is wider than people are reading
15 it.

16 It would be helpful -- it would be very
17 helpful to know that.

18 Second, I wanted to take a crack at your
19 question about (j). And I don't know if I have a
20 good answer about the network situation.

21 But I think the concern that we're
22 primarily getting after here is if you think about
23 the little message bank. So I think one
24 interpretation of (j) is that the computer or the
25 computer system or whatever you want to call it

1 there is the bank itself. And Matt went out and
2 bought the bank and he's the owner of it, and
3 that's, of course, the argument that we can make.

4 I think the concern, though, is when you
5 look to that analogy that Ms. Smith brought up in
6 the legislative history that the TPM that's on
7 that system is not protecting Mr. Stanislav's
8 property; it's protecting the computer software.

9 And the question is: Who owns the
10 software?

11 Now, we might make the argument that we
12 own the software because we bought it. But I'm
13 willing to bet that the company that sells that
14 makes the argument that they just licensed the
15 software and that we're not the owner of it and,
16 in fact, that software is not a computer system at
17 all and what we're engaged in is not the act of
18 accessing a computer system but that we're engaged
19 in the act of accessing a copyrighted work.

20 And so I think that's the ambiguity that
21 has led in the past to the office granting some
22 clarity on this by granting an exemption.

23 So I think we would fully agree with
24 your interpretation if we're in court trying to
25 defend this. And we would absolutely push for the

1 broadest possible interpretation of (j). But when
2 we're trying to advise folks, we have to
3 acknowledge it's amenable to multiple
4 interpretations. And that's why we are seeking
5 some clarity.

6 MS. CHARLESWORTH: Yeah. Just for the
7 record, I mean, in exploring the meaning of this,
8 we have not come to any conclusions about the
9 meaning of (j). And I think my colleague was
10 asking --

11 MR. DAMLE: I was exploring potential
12 readings.

13 MS. CHARLESWORTH: Potential reading.

14 MR. REID: I will do my best to unhear
15 that.

16 MS. CHARLESWORTH: Your point is well
17 taken, Professor Reid. You know, we'll think
18 about that carefully.

19 But in exploring the meanings, we're
20 trying to push counsel to kind of give us your
21 explanation.

22 MR. REID: Right.

23 MS. CHARLESWORTH: So this transcript
24 shall not constitute a record of how we're
25 interpreting (j). We may get there someday. We

1 hope -- we hope to, you know, provide some
2 clarity, obviously. But for now, we're having a
3 discussion.

4 MR. REID: Well, if there's one other
5 thing I could put out there, I would direct you to
6 think as you're thinking about this
7 interpretation, for the standard in 1201(a) for
8 granting an exemption, which is the likelihood of
9 adverse effects.

10 And I think what you've heard today is
11 that there are likely adverse effects because of
12 the uncertainty around this. So I don't think you
13 have to come to an ironclad conclusion about what
14 Section 1201(j) says or doesn't say in order to
15 grant this exemption. And I don't think the
16 office has ever done that in the past.

17 So if your conclusion looking at this is
18 that it's amenable to a couple of different
19 readings but that security researchers are going
20 to be chilled by the fact that it's not clear,
21 then you need to grant the exemption. And that's
22 what the office has done in the past, and we'd
23 encourage you to do so again this time.

24 MS. CHARLESWORTH: Okay. Back to -- oh.
25 Professor Bellovin.

1 MR. BELLOVIN: I was just going to
2 follow up on what Professor Reid said and perhaps
3 explain it in a slightly different way.

4 As I read Section (j), it is -- the
5 scenario contemplated is "I'm an employee of, say,
6 a bank. I want to protect my own computer
7 system." Attacking some other bank, that may or
8 may not be a violation of the Computer Fraud and
9 Abuse Act. No one here on this side of the table
10 is advocating doing that irresponsibly. That's
11 not the issue.

12 But if it's my bank, if I find a flaw,
13 yeah, I might be able to take protective measures
14 or I might not, depending on what the situation
15 is. Even the most sophisticated users would have
16 a very hard time remediating a flaw in something
17 like an iPhone, which is a very closed system.

18 But what we are talking about as
19 security researchers is not the very narrow
20 question of who owns a particular device but
21 vulnerabilities not in the device but in the
22 software -- which, as Professor Reid noted, we
23 arguably do not even own, according to the license
24 agreements we have to click through every time we
25 open up a toy box or something -- and it's -- the

1 issue is not so much the flaw in our particular
2 copy but the flaw in the class of copies, of which
3 there may be hundreds of millions out there, and
4 which manufacturers often don't want -- they may
5 or may not want to hear about it. They certainly
6 don't want anybody else to hear about it.

7 And that is where the chilling effect is
8 taking place, not by copy, where if the flaw is
9 serious enough I will just not use it, but
10 everybody else, the hundreds of millions of other
11 instances of that software out there that are all
12 owned by the manufacturer and licensed to
13 consumers and companies that have to be protected.
14 That is what we're trying to solve the problem of.

15 MS. CHARLESWORTH: Okay. Thank you,
16 Professor.

17 Mr. Stallman, were you --

18 MR. STALLMAN: I just had one more point
19 on 1201(j), and then I'll leave the rest for
20 questioning.

21 But the other deficiency with it is
22 references to violation of other applicable laws,
23 specifically including 18 U.S.C. 1030.

24 In our reply comments, we included a
25 statement on legal impediments to cybersecurity

1 research that was signed by 35 noted security
2 research experts. An additional 14, I think, have
3 signed on to that comment now just because it was
4 around and they were interested in it.

5 And so I would like to submit that for
6 the record.

7 But the general point is that, because
8 Section 1201(j) includes these other provisions
9 like the CFAA, like the Wiretap Act, like the
10 Stored Communications Act, which are themselves
11 uncertain with respect to whether or not research
12 violates those statutes, 1201(j) has the
13 unfortunate effect of sort of compounding and
14 amplifying the uncertainty and the legal risks
15 that already exist in this law.

16 And I don't think it's a satisfying
17 answer to say that, well, just because there's
18 other, you know, legal murkiness around this issue
19 we shouldn't address this one because I think this
20 is -- this is one opportunity that the office can
21 remove one of the -- the most significant
22 impediments but also send a clear signal that this
23 is -- this is an area that other -- that the
24 Congress and other agencies should be looking at.

25 MS. CHARLESWORTH: Mr. Stallman, on the

1 updated exhibit, is that the exact same comment?

2 MR. STALLMAN: Yes, it is.

3 MS. CHARLESWORTH: It just has
4 additional signatures?

5 MR. STALLMAN: Additional signatures,
6 yes.

7 MS. CHARLESWORTH: So people previously
8 have had an opportunity to --

9 MR. STALLMAN: Yes.

10 MS. CHARLESWORTH: -- see the comment?

11 MR. STALLMAN: Yes.

12 MS. CHARLESWORTH: Okay.

13 MR. STALLMAN: The text is entirely
14 unchanged.

15 MS. CHARLESWORTH: All right. Well,
16 we'll -- because it's the same text, we'll accept
17 that as Exhibit 11.

18 MR. STALLMAN: Thank you.

19 MS. CHARLESWORTH: Has it been marked,
20 Steve? Okay.

21 (Whereupon, Exhibit No. 11 was marked
22 for identification.)

23 MS. CHARLESWORTH: So that will go into
24 the record with the additional signers.

25 MR. STALLMAN: Thank you.

1 MS. CHARLESWORTH: Thank you.

2 Okay. This is -- this is a very long
3 panel. I see Mr. -- don't get overly excited.

4 We were wondering if people might like
5 truly a five -- when I say "five-minute," a five-
6 minute break just to stretch their legs before we
7 begin with the opposition.

8 And, you know, people are nodding yes.
9 So it is -- what time do you -- my watch is --
10 11:15. So if we can come back at 11:20, and we'll
11 resume the discussion.

12 Thank you.

13 (Whereupon, a short recess was held.)

14 MS. CHARLESWORTH: Okay. We're back
15 with class 25, software and security research. And
16 I'm going to turn to -- now to Mr. Troncoso.

17 MR. TRONCOSO: Thank you. Proponents
18 characterize class 25 as an exemption to enable
19 good-faith security testing, and we totally
20 support this goal. I also wanted to agree with
21 something that Professor Green said in his opening
22 statement, that we really are surrounded by the
23 good guys and we have a big interest in working
24 with the academic and independent research
25 communities to advance security interests.

1 However, we also need to recognize the
2 fact that any possible exemption that is granted
3 in the course of this proceeding also has the
4 potential to be exploited by the bad guys. And so
5 I just wanted to frame my comments with that.

6 BSA members recognize that user trust is
7 indispensable and that that trust must be earned.
8 BSA members also recognize the importance of
9 collaborating with the independent research
10 community, and they do so every day.

11 BSA members are, however, extremely
12 worried about one particular aspect of this class,
13 the specific authorization for researchers to make
14 disclosures about vulnerabilities based upon the
15 researcher's sole judgment before the software
16 developer has had an opportunity to remedy the
17 problem.

18 It's a sad fact that bad actors are
19 relentlessly searching for vulnerabilities that
20 they can profit off of from the software that all
21 of us rely on in our daily lives. We believe
22 specifically authorizing zero-day disclosure
23 practices through this rulemaking may well enable
24 exploitation of vulnerabilities to engage in
25 identify theft, financial fraud, and other serious

1 threats to our nation's critical infrastructure.

2 The objective of this proceeding must be
3 to promote security research in a manner that is -
4 - that thwarts those malefactors without creating
5 unintended consequences.

6 Both Congress and the administration are
7 in the midst of vigorous debates on these very
8 issues. Congress is currently considering
9 legislation on information-sharing proposals aimed
10 at creating incentives for parties to share threat
11 and vulnerability data both with private parties
12 and the government.

13 BSA strongly supports enactment of these
14 bills.

15 At the center of the congressional
16 debate is how best to create those incentives
17 principally by limiting liability without
18 unintended consequences. The Obama administration
19 is also considering important policy initiatives
20 on vulnerability information disclosures.

21 The Department of Commerce recently
22 announced that it is considering implementing
23 export controls on the tools used to hack systems
24 to discover vulnerabilities. The Commerce concern
25 is, again, about balance; how to responsibly

1 disseminate tools while guarding against their
2 falling into the hands of persons with bad
3 intentions.

4 Nearly 20 years ago, Congress struggled
5 with these same considerations when enacting the
6 DMCA. Congress enacted exceptions to the
7 circumvention prohibitions to promote security
8 research but included careful checks and balances
9 on the ability of people to make ill use of these
10 exceptions.

11 Proponents of class 25 argue that
12 ambiguity within these statutory exemptions are
13 having chilling effects on the very type of
14 research they were intended to promote. Were
15 proponents merely seeking narrow classification to
16 these provisions, we would not oppose their
17 efforts.

18 However, proposed class 25 does much
19 more than that. The reality is that proponents
20 are seeking an exemption that is both broader than
21 existing statutory exemptions but which contain
22 none of the important safeguards that Congress
23 deemed important.

24 Consistent with congressional intent, as
25 reflected in the DMCA's current statutory

1 exceptions, we believe that class 25 should be
2 amended to permit circumvention only when the
3 software has been lawfully obtained, the
4 researcher has made a good-faith effort to obtain
5 authorization from the owner of the system or
6 network, circumvention is carried out solely for
7 the purpose of good-faith testing, and the
8 information derived from the testing is used
9 primarily to promote the security of the software
10 and maintained in a manner that does not
11 facilitate copyright infringement or any other
12 violation of applicable law, including the CFAA.

13 Most importantly, the disclosure of
14 vulnerability information must be done judiciously
15 consistent with the facts of the specific
16 situation in ways that avoid unintended
17 consequences.

18 We believe that judicious disclosure
19 requires vulnerability information to be first
20 shared with the entity best placed to fix it,
21 namely the developer, and with enough time to cure
22 the problem before it is disclosed more broadly.

23 The concurrent disclosure standard
24 proponents advocate would exacerbate the risk to
25 the public by affording bad actors a window of

1 opportunity to exploit vulnerabilities before
2 they've been patched.

3 This isn't a speculative concern.
4 Unfortunately, there is already a thriving market
5 for black market -- in the black market for
6 security research regarding zero-day
7 vulnerabilities.

8 Should you determine that a broad
9 security exemption is warranted, we urge that you
10 tailor the class in a manner that is consistent
11 with congressional intent and that you are mindful
12 of the broader national cybersecurity policy
13 debate that is now under way in Congress and
14 within the administration.

15 Most importantly, the goal must be to
16 help good-faith researchers here today and not
17 inadvertently to help bad actors.

18 Happy to answer any questions that you
19 have.

20 MS. CHARLESWORTH: So on -- on the
21 disclosure, we've heard a lot about that. I mean,
22 what -- if we were to -- you know, the
23 congressional standard, as you know -- or the
24 standard that's in 1201(j) is that -- the
25 complaint is that it's too opened-ended.

1 MR. TRONCOSO: Mm-hmm.

2 MS. CHARLESWORTH: You know, you're
3 looking back. I mean, do you have any specific
4 proposals in terms of how to address -- when you
5 say, you know, "notify the manufacturer first," is
6 there a time constraint before you can
7 disseminate? Or how would you -- if you -- if you
8 were going to address this in an exemption, how
9 exactly would you do that?

10 MR. TRONCOSO: Mm-hmm. Well, I mean, I
11 think, as a preliminary matter, you would first
12 need to make the determination that there has been
13 a substantive chilling effect on these research
14 activities. And there's a lot of research going
15 on.

16 Obviously, I take everyone at their
17 word. I think that, on the edges, there certainly
18 is some chilling. But I think if you look at the
19 market right now, BSA-member companies have a big
20 interest in partnering with the independent
21 research community. And many of them are actively
22 trying to incentivize that by offering rewards,
23 either financial or reputational, to those who
24 provide information about security vulnerabilities
25 but do so in a responsible manner.

1 And typically, that just means providing
2 the vendor with enough time to issue a patch
3 before the security researcher makes that -- makes
4 a public disclosure about the specifics of that
5 vulnerability.

6 MS. CHARLESWORTH: And how much time is
7 that?

8 MR. TRONCOSO: You know, there is not
9 really a set time. And I'm sorry I can't give you
10 an easy answer on that.

11 The reality is that every vulnerability
12 is different, and the fix to every vulnerability
13 may take a different amount of time.

14 You know, particularly with enterprise
15 software, when our member companies are evaluating
16 patches to vulnerabilities that have been
17 identified, they need to spend a lot of time with
18 that patch to ensure that it's not going to create
19 some other type of vulnerability down the line.
20 And because enterprises are so complex and system
21 upon system upon system, that can just take a lot
22 of time.

23 Some patches are easy to -- easy to get
24 out, but others aren't. So I think that we'd be
25 probably uncomfortable with a fixed deadline for,

1 you know, disclosure for those reasons.

2 MS. CHARLESWORTH: Do your companies --
3 I mean, you sort of spoke about this a little bit.
4 But, I mean, how -- how many of your members -- or
5 what percentage of them actually authorize
6 security research? Do you know?

7 MR. TRONCOSO: I don't know the exact
8 number. I know that the trend is for software
9 companies to do that, but I don't know how many do
10 in a sort of official capacity. Some of them
11 probably also work sort of more behind the scenes.

12 But there's certainly many of them that
13 have, you know, very visible programs that are
14 advertised on their websites about that.

15 MS. CHARLESWORTH: Okay.

16 MS. SMITH: Do your members have any
17 specific concern about the dissemination or
18 discovery of trade secrets in security research
19 that's unauthorized?

20 MR. TRONCOSO: I think, absolutely, that
21 would be a concern of our member companies.

22 MS. SMITH: Okay. I mean, have you seen
23 any specifically? Because I think you said you
24 would be okay with the exemption if it was
25 narrowed from the proposal?

1 MR. TRONCOSO: Mm-hmm.

2 MS. SMITH: But I'm wondering if -- you
3 know, how could we address this concern or how
4 realistic, you know, or palpable is this concern?

5 MR. TRONCOSO: I mean, I think that you
6 would want to build in sort of the standard that I
7 had referred to earlier, that it couldn't involve
8 any other violation of applicable law. And so
9 that would apply to sort of disclosure of trade
10 secrets as well.

11 MS. SMITH: Okay. So that would satisfy
12 the concern?

13 MR. TRONCOSO: That particular concern.

14 MS. CHARLESWORTH: Okay. Mr. Lightsey?

15 MR. LIGHTSEY: Yes. Thank you. Good
16 morning.

17 I'll just begin by noting that my
18 comments are directed solely with regard to any
19 impact that the proposed class might have on the
20 automobile industry. I don't purport to address
21 anything beyond the impact on automobiles.

22 So today GM vehicles include, on
23 average, 30 purpose-built electronic-control
24 units, or ECUs, that control functions in the
25 automobile ranging from the radio to vital engine

1 and safety functions.

2 These ECUs control functions like engine
3 controls, braking, speed, steering, air bags, and
4 other very important features for the safety of
5 the occupants in the vehicle.

6 These ECUs -- the software in these ECUs
7 is protected by technological protection measures,
8 or TPMs, that, if circumvented, could present real
9 and present concerns for the safety of the
10 occupants of the vehicle as well as the compliance
11 of the vehicle with regulatory and environmental
12 requirements.

13 So TPMs play a vital role in the overall
14 security and safety design of the vehicle.

15 Now, with regard to the chilling effect,
16 particularly in the automobile industry, the
17 proponents have not presented any evidence that
18 there has been any chilling effect whatsoever. In
19 fact, to the contrary.

20 And that's because the automobile
21 industry is -- has every incentive to encourage
22 responsible security research and does so. We
23 have, as we said in the class 22 proceeding,
24 relationships with various independent security
25 researchers, academics institutions. We

1 participate in various industry forum, including
2 SAE and others. We attend meetings of the
3 security research industry, such as the Black Hat
4 conference and the DEF CON conference. We do --
5 we do every -- we engage in various efforts with
6 DARPA.

7 And so we certainly do our part to
8 encourage responsible security research into the
9 software in our systems.

10 And our concern is that, if the broad
11 exemption, as proposed, is granted, that the
12 ability for automobile manufacturers to control
13 that research and to have the opportunity to fix
14 vulnerabilities before they're widely disclosed
15 would be severely limited and could thus create
16 safety concerns.

17 Thank you very much.

18 MS. CHARLESWORTH: Thank you.

19 Mr. Troncoso, I had a question that I
20 neglected to ask you earlier.

21 In some of your papers, in your filing
22 or the filing, I think, of BSA, it mentioned that
23 the research should be limited to vulnerabilities
24 caused by access controls.

25 Do you -- can you comment on that? And

1 is that -- I didn't hear you say that just now.

2 MR. TRONCOSO: Yeah. I think that when
3 -- we were talking about the fact -- those are the
4 only extensions, as far as I know, that the
5 Copyright Office has granted in the past, that
6 they were sort of narrowing tailored to specific
7 types of access controls that were creating
8 security vulnerabilities.

9 But the class that we're looking at here
10 is extraordinarily broad and would apply to
11 virtually any type of software.

12 So, you know, I would need to go -- I
13 don't have the filing in front of me. But I --

14 MS. CHARLESWORTH: But is it your
15 position that -- I mean, at least in one of the --
16 one part of your papers, I think I saw that you
17 were okay with a narrow exemption in this area,
18 but it should be limited to vulnerabilities caused
19 by access controls.

20 Am I -- is that an incorrect
21 understanding of your position?

22 MR. TRONCOSO: No. We would certainly
23 be comfortable with a narrow exemption like that.

24 MS. CHARLESWORTH: Right. But are you
25 saying you -- there's no version of an exemption

1 that could be broader than that that you'd be
2 comfortable with?

3 Because that's a fairly -- that's a
4 fairly significant limitation.

5 MR. TRONCOSO: Okay. Fair enough.

6 I think that our overriding concern is
7 about the disclosure issue, and that's certainly
8 what is motivating our participation in this
9 proceeding.

10 And to the extent that that can be
11 addressed and that congressional sort of intent
12 underlying the existing statutory exemptions can
13 be integrated, we would be comfortable with an
14 exemption.

15 MS. CHARLESWORTH: An exemption that was
16 broader than just vulnerabilities that are
17 specific to the access controls themselves?

18 MR. TRONCOSO: That's correct.

19 MS. CHARLESWORTH: Okay. Thank you for
20 that clarification.

21 Okay. Going back to the disclosure
22 issue -- well, I think there are a few issues that
23 we've identified. One is this sort of issue of
24 the specter of, you know, are you looking at a
25 consumer good -- like the piggy mailbox this

1 morning were you can kind of take it and look at
2 and it work with it in a way that's probably not
3 that risky, hopefully, to anyone else?

4 You know, or are you talking about
5 nuclear power plants, I mean, that specter where
6 you'd be hacking into, like -- or a plane's
7 operating system as the plane is operating?

8 And I'd really be curious to know from
9 the researchers, I mean, how to think about that
10 issue and address it in practical terms.

11 I mean, I don't think there's a huge
12 record here of needing to, you know, look at live
13 nuclear power plants and things. But, I mean, I
14 don't want to -- obviously, that's also a security
15 concern, and I don't want to say it's not.

16 But, I mean, how should the office be
17 thinking about this question and the
18 concern that, say, publishing research about how
19 to break into a system where the breach
20 of -- where the breach could be
21 catastrophic, let's say, or very serious for the
22 public?

23 I mean, how should we think about that?

24 Is that -- Dr. Green? Did you want to
25 comment on that?

1 MR. GREEN: Sure. So I think there are
2 two issues here.

3 One is: Should you be performing
4 security testing or research on live, active
5 systems?

6 That's obviously something that can be
7 very dangerous, and you should use extreme
8 restraint with that.

9 However, there are other laws that
10 directly apply to that. For example, the CFAA is
11 a law that is, as far as I can see, specifically
12 designed to deal with a case of people accessing
13 online systems in unauthorized ways. So I have
14 never viewed the DMCA as being something that
15 specifically applies to that case. Of course, I'm
16 not a lawyer. That's just my interpretation as a
17 researcher.

18 Now, having said that, there are --
19 certainly, there are things that -- I mean, the
20 question then is: Is it something that you should
21 be allowed to do? Is it something that we should
22 be -- should we be using Section 1201 as a way to
23 prevent people from doing research on these types
24 of systems? Does that benefit us as a society?

25 I think the answer is that clearly it

1 does not benefit us because, you know, we have
2 access to a -- we know that there are a number of
3 systems, such as control systems, that, whether
4 you're accessing them in real time or whether
5 you're accessing separate copies, the results of
6 the experimentation can lead to vulnerabilities
7 that cause major safety issues in things like
8 nuclear power plants.

9 So the value of performing that research
10 and, you know, properly disclosing and getting
11 those vulnerabilities fixed is very, very high.

12 MS. CHARLESWORTH: I mean, I can agree
13 with you there. But, I mean, I saw a news report
14 recently about someone who allegedly -- I hear
15 laughter -- hacked into -- but it's not funny to
16 me since I spend a lot of time on airplanes --
17 hacked into a live, operating airplane system.

18 And now they may be doing it for a good
19 -- for what they perceive to be good purposes.
20 But, you know, aside from the fact that, you know
21 -- well, I mean, a security researcher is also not
22 a perfect person. As smart as you all are, I
23 mean, you could also make a mistake when you take
24 over the airplane to operate -- I mean, this is
25 getting -- it sounds a little absurd, but if I

1 believe the report, someone did that.

2 And, yes, on the one hand, exposed a
3 flaw. But on the other hand, if I were riding on
4 that plane, I would -- would not -- I mean, I
5 would be uncomfortable knowing that it was being
6 piloted by someone who, you know, may know less
7 about piloting an airplane than the pilot.

8 So anyway, I'm just wondering -- I mean,
9 are you saying -- would you be willing to limit
10 this so that -- at least for purposes of 1201
11 where we're talking about not live systems and
12 maybe that question should be debated in Congress
13 in terms of how to perform security research on
14 nuclear power plants and things of that nature?

15 MR. GREEN: So I'm going to leave the
16 legal aspects of that response to my colleague
17 here. But I am going to say just -- I think I
18 speak for all of the security researchers here
19 when I say that that story is not something that
20 we endorse.

21 MS. CHARLESWORTH: Thank you. That's
22 good to know.

23 MR. GREEN: No ethical researcher should
24 be working on live systems like that, and we -- if
25 it happened, we're very unhappy about it.

1 MS. CHARLESWORTH: Okay. Thank you for
2 that.

3 MR. REID: And I just wanted to chime in
4 too and say, in addition to distinguishing that
5 particular story, I think the vast majority of the
6 research that we're talking about here and,
7 indeed, I think all of the research that we care
8 about is responsible work that's aimed at fixing
9 problems like these in a safe way.

10 And so I think the anecdote of that
11 story shouldn't -- I hope won't color the office's
12 judgment too much on this.

13 The other thing I would throw out here
14 is --

15 MS. CHARLESWORTH: Well, wait a second.
16 But you're just -- I mean, that's just circular.
17 It's saying, "Well, we want an exemption that
18 allows ethical stuff, and we don't think that's
19 ethical." But, you know -- but, I mean, I said
20 this in L.A. in a different context. I mean,
21 we're trying to -- part of our job here is, if we
22 -- if we do go forward and grant some sort of
23 exemption, there needs to be enough information
24 and enough sort of -- a little bit of line-drawing
25 in there so that you're notifying the public of

1 what they can and can't do.

2 MR. REID: Sure.

3 MS. CHARLESWORTH: And also, I think,
4 assuaging fears to some extent of people who might
5 be worried that it would be used in ways that
6 were, say, dangerous. I mean, I -- you know, so I
7 -- saying -- you know, often we get that response.
8 It's just we're saying it should be lawful. We're
9 saying it should be ethical.

10 But at the same time, we're
11 looking at the record here and we're trying to
12 consider some potential limitations or
13 narrowing so that people feel that the exemption
14 would be one that's consistent with congressional
15 intent and the goals of the proceeding.

16 So if you could maybe speak a little bit
17 more -- I mean, so I'm -- basically, it's like,
18 "Are we willing to get rid of -- to
19 exclude live systems from this exemption?"

20 I don't think there's much of a record -
21 - I will say that -- and to support the idea that
22 you would need that and, you know -- I'd be
23 interested to know whether that's something that
24 the researchers could concede may not be necessary
25 at least at this moment in time for this exemption

1 that's sought.

2 MR. REID: I mean, I guess the -- the
3 other thing that I'd urge you to consider is that
4 however this gets treated in this proceeding,
5 whether you choose to include live systems or not
6 to include live systems, as Professor Green
7 mentioned, there are a number of other laws that
8 deal with this sort of thing. And I think a lot
9 of the collateral concerns that folks have raised
10 -- you know, tampering with vehicles, tampering
11 with medical devices, tampering with live
12 airplanes -- are illegal under a whole bunch of
13 laws.

14 And I think the question you ought to be
15 asking yourselves is: Are we -- is the DMCA the
16 last line of defense to protect airplanes? Are we
17 relying on copyright law to protect the security
18 of airplanes?

19 MS. CHARLESWORTH: Apparently so,
20 according to some.

21 MR. REID: Because I think, as a matter
22 of policy, A, we're not. And, B, if we were, that
23 would be -- that would be deeply troublesome. And,
24 C, we're getting so far away from the reason the
25 DMCA was enacted, which is to protect the

1 commercial exploitation of copyrighted works from
2 copyright infringement.

3 There's nothing that I could tell in the
4 report about the airline incident that indicated
5 anything about copyrighted software. There's
6 nothing about a technological protection measure.
7 There's nothing about circumvention. And in the
8 affidavit from the FBI, there's no citation to the
9 DMCA or any provision of the Copyright Act.
10 There's a citation to Section 1030.

11 So I think, to the extent that there are
12 concerns about this, there are a number of other
13 both legal and policy venues in which they can be
14 addressed. And I don't think the office needs to
15 be worried about enabling behavior that's illegal
16 under other -- under other laws because there's
17 still -- the behavior is still going to be illegal
18 under those other laws.

19 And I think what we're trying to get at
20 here is there are complicated contours to this
21 discussion, and there are discussions that should
22 happen in other venues. Obviously, folks have
23 raised concerns about the EPA and the FDA and that
24 sort of thing. And I think we're in support of
25 having those discussions at those venues and in

1 the context of those laws and policies.

2 But I think what we're trying to press
3 for here is that copyright law is not the place to
4 do it and that you don't need to and that the DMCA
5 and Section 1201 don't require you to.

6 MS. CHARLESWORTH: Okay. Thank you.

7 Professor Bellovin?

8 MR. BELLOVIN: I want to thank you for
9 focusing on copyright laws, about half of what I
10 was going to say. I would -- the only thing I
11 would add in that vein is we are here precisely
12 because we want to make certain that we're in
13 compliance with the law. We are very much
14 concerned with avoiding breaking laws. It's
15 exactly why we want this exemption. We don't want
16 to violate the copyright law. We don't want to
17 violate the CFAA. We don't want to violate the
18 airplane hijacking laws.

19 As a -- you know -- but just returning
20 to the purely technical issue of copyright
21 infringement. It is almost never a concern -- in
22 fact, I'm hard-pressed to think of any example
23 where copyright infringement becomes a concern
24 unless you have a copy of the system.

25 If this guy who allegedly tried to hack

1 into an airplane in flight -- thank God. I fly a
2 lot. I don't like hearing this either.

3 In order to be able copy, say, Boeing's
4 software -- which would be copyright infringement
5 -- he first had to hack into something. As a
6 pragmatic matter, if I am testing a system for
7 security flaws in a way that could possibly
8 involve copying, I have to have the physical thing
9 in my possession because that's where the code is.
10 That's where the copyrighted material is.

11 You know, this is not a CFAA exemption
12 request. That may be a good thing. I have
13 opinions on that, but I'm not going to go into it.

14 But as a pragmatic matter, infringing
15 copyright, circumventing a protection on
16 copyright, circumventing a technological measure
17 that's protecting copyright pretty much requires
18 that it be your device because that's how you have
19 access to the code or the circuit boards or
20 whatever that is the actual copyrighted material.

21 And it --

22 MS. CHARLESWORTH: Well -- I'm sorry.
23 You're so much more skilled in this area than I
24 am. But couldn't you hack into someone's system
25 through the Internet?

1 MR. BELLOVIN: But then you have to hack
2 in first. You have to first violate the CFAA to
3 get at the system before you can get at the
4 copyrighted material. The larger violation there
5 is the hacking.

6 And I think a more probable case,
7 certainly one we have seen, is not involving the
8 DMCA, but I'm going to hack into a company in
9 order to steal their source code, their trade
10 secrets, what have you. And this is not protected
11 by the sort of technological measures that the
12 DMCA bars circumvention of. This is protected by
13 ordinary computer security controls and enterprise
14 security controls and firewalls to keep bad guys
15 out of my system.

16 It's not -- you know, the DMCA was
17 intended to protect devices that contained code or
18 books or what have you that has been legitimately
19 purchased that you're trying to prevent extraction
20 of, reproduction of in violation of the Copyright
21 Act. It's not intended to be a CFAA supplement.

22 And, again, as a technical matter,
23 that's rarely the way. You have to go break
24 something else if it's somebody else's system,
25 violate the CFAA before you can get to the

1 copyrighted code. And that's rarely the way that
2 copyrighted or otherwise protected material is
3 stolen because of a hack.

4 MS. CHARLESWORTH: Okay. Thank you.

5 Professor Matwyshyn?

6 MS. MATWYSHYN: Just very briefly, the
7 exact facts of the incident that you're
8 referencing are still somewhat in dispute. And so
9 time will give us a better sense of exactly what
10 happened.

11 But at present, I think the lack of
12 support for such conduct that you're seeing from
13 the researchers representative, large portions of
14 the security community are absolutely not rallying
15 around the conduct of this individual.

16 MS. CHARLESWORTH: Well, I would hope
17 not.

18 MS. MATWYSHYN: They are not. I give
19 you my assurance. This is a deeply troubling turn
20 of events.

21 So the norms of the security research
22 community are not in line with this type of
23 conduct.

24 MS. CHARLESWORTH: Yeah.

25 MS. MATWYSHYN: And in that type of a

1 situation, the homicide laws are the first line of
2 defense. And that is the severity of the problem.

3 And so the -- whether a TPM was
4 circumvented in the process of killing hundreds of
5 innocent people, we hopefully will never need to
6 inquire on that scale.

7 MS. CHARLESWORTH: Okay. Yes. I mean,
8 I appreciate all the comments about, you know, the
9 relationship between copyright law or the lack
10 thereof and what we're talking about.

11 But because of the way the law is
12 written, these are -- I said this in L.A. too --
13 these are the issues that have come to the table,
14 and so we have to consider them.

15 And, Professor Blaze, your turn.

16 MR. BLAZE: So first of all, I mean, let
17 me add my voice to the chorus that condemns
18 tampering with live safety, critical systems. I
19 think nobody -- nobody advocates that here. And I
20 -- certainly not I.

21 And as a frequent flyer, I was as
22 horrified as anyone at the possibility of this
23 sort of tampering, although all the facts are
24 quite murky at this point.

25 I wanted to return to the other issue

1 that you had asked us to talk about, which was
2 disclosure.

3 You know, I want to not give short
4 shrift to the -- the purpose of disclosure is not
5 -- is partly to help have these security
6 vulnerabilities that might be discovered repaired.
7 But there's a second and, I think, equally
8 important purpose, which is warning consumers
9 against defective products.

10 For example, in the -- I'm not quite
11 sure what it's called -- this odd little mailbox
12 pig.

13 MS. CHARLESWORTH: Exhibit 10, I think.

14 MR. BLAZE: Yeah. The mailbox voicemail
15 pig.

16 You know, certainly, if I were a parent
17 with one of these devices, I think, you know, even
18 before it's fixed, if this had vulnerabilities
19 that could expose my child to danger, I would want
20 to know about that and remove it. And disclosure
21 to the public is really the only way to achieve
22 that even if it's at the expense of some
23 embarrassment to the vendor.

24 So I want to make sure that we give
25 adequate consideration to the benefit of the

1 security research and scientific process, not
2 merely considering the stakeholder as being the
3 developer of the software but also the users of
4 the technology more broadly.

5 MS. CHARLESWORTH: Thank you.

6 Mr. Lightsey?

7 MR. LIGHTSEY: Yes. I'd just like to
8 say, once again, with regard to the automobile
9 industry, there's been absolutely no evidence of
10 any chilling effect on security research.

11 And given the dramatic consequences that
12 we're concerned about here in terms of people's
13 safety and lives, we feel very strongly that the
14 proponents have not met any burden that they might
15 have of showing a need for an exemption here.

16 And by simply saying, "Well, there are
17 other laws and regulations and regulatory bodies
18 out there that address these concerns," it is not
19 sufficient in this context as well.

20 We feel that the DMCA is a relevant
21 protection, and we encourage the ability to engage
22 with the security -- responsible security
23 researchers and to have the opportunity to fix the
24 vulnerabilities that they can find.

25 Thank you.

1 MS. CHARLESWORTH: Thank you, Mr.

2 Lightsey.

3 Mr. Troncoso?

4 MR. TRONCOSO: Returning back to

5 everyone's favorite pink little pig example, I

6 just wanted to point out -- thank you -- Mr.

7 Stanislav, when he explained sort of what happened

8 to him as he was researching that vulnerability,

9 if I recall correctly, he explained that he

10 reached out first to the manufacturer and, you

11 know, notwithstanding the bluster that sort of he

12 may have received at first, ultimately he was able

13 to work with the manufacturer to ensure that that

14 vulnerability was fixed. And he didn't -- and Mr.

15 Stanislav did not disclose the information about

16 that vulnerability until after it was fixed.

17 And I think that that sort of gets to

18 the -- to the norm that we're seeing even amongst

19 the researchers in this room that, you know, it is

20 consistent with what software companies' interests

21 are, which is protecting consumers from these

22 vulnerabilities.

23 And I'll also point out that, in

24 Professor Green's filing -- his initial filing --

25 and his sort of research addendum at the end of

1 his filing, he indicates that he always provides
2 disclosure to software companies before disclosing
3 vulnerabilities to the public. And that really is
4 a key issue for us and one that is critical to
5 safety of the public.

6 Thanks.

7 MS. CHARLESWORTH: Thank you.

8 Professor Green, do you want to respond
9 to that and whatever else you had to say?

10 MR. GREEN: Sure. I'd like to say that
11 I always attempt to provide disclosure to software
12 companies. In some cases, it's not possible. And
13 I gave an example of a vulnerability where there
14 were thousands of websites and we simply couldn't
15 notify everybody.

16 The other issue I'd like to bring up
17 with disclosure is that sometimes you notify --
18 you disclose somebody -- a software company of an
19 issue, and they are not able to properly remediate
20 it, tell you that there's no fix, or they tell you
21 that the fix that they can provide will take a
22 year.

23 At that point, you have the obligation
24 as a researcher to look at the end users, the
25 consumers affected. And that has to affect your

1 calculation quite a bit.

2 For example, Android telephone -- this
3 is one. But Android telephones are rarely updated
4 by carriers. So if you notify Google of a
5 vulnerability, they will make a patch. But the
6 probability that it actually gets out to consumers
7 is very low -- to most consumers. Ninety percent
8 of consumers can be vulnerable a year later.

9 So you have to make a lot of calculation
10 about how you disclose things based on what's
11 right for consumers and not what's right for
12 software companies.

13 MS. CHARLESWORTH: Okay. I think it was
14 Professor -- oh, I'm sorry. Mr. -- yeah. I
15 couldn't -- sideways to me.

16 MR. STANISLAV: The pig keeps getting in
17 my way.

18 So to your point, sir, the three minutes
19 I had to explain my situation for multiple things
20 was -- I was a little short.

21 In the case of this specific device --
22 and also this device as well -- in order to
23 disclose these issues --

24 MS. CHARLESWORTH: And that's -- sorry.
25 For the record, we're talking -- are those both

1 now in Exhibit 10, the devices?

2 Oh, okay. All right. Exhibit 12? Yes.

3 MR. STANISLAV: With both items in
4 Exhibit 12 then. Both of these were reported
5 through the help desk system of that -- of the
6 organizations because there was no front door for
7 me to access. I had to go through multiple days
8 just to convince the help desk employees that
9 these were issues I needed help with and to triage
10 them up the chain to someone who could address
11 them directly.

12 I actually had a help desk ticket closed
13 on me for this specific camera device and had to
14 reopen a new help desk ticket just to continue
15 dialogue.

16 Specifically, however, with this device,
17 the only reason that these issues finally got
18 solved after about a -- offhand, about a month and
19 a half -- was because my company at the time was
20 going to disclose the vulnerability through public
21 channels because there were no -- there was no
22 progress on getting these issues solved.

23 At that point, a reporter reached out to
24 the vendor. The vendor said they had never heard
25 from a researcher about any issues. And then I

1 received a reply from the CEO of this company that
2 same day on the e-mail thread I had been having
3 with her addressing, "Oh, maybe we should have a
4 phone call to discuss this issue if you are still
5 pursuing it."

6 MS. CHARLESWORTH: And that's the pig
7 device?

8 MR. STANISLAV: Yes.

9 MS. CHARLESWORTH: Okay.

10 MR. STANISLAV: So I certainly -- there
11 are many great vendors out there. The BSA
12 represents many of the vendors that do work really
13 well with security researchers. Microsoft being
14 one of them, for sure.

15 However, these companies represent the
16 companies that most of the products you are buying
17 are from. They are not from the tier-one
18 providers.

19 The Internet of things is generated from
20 innovators, from entrepreneurs, from people on
21 crowdfunding sites like Kickstarter. These people
22 do not have large legal teams that understand
23 complex legal situations. They will fight back
24 with whatever means they have to shut you up to
25 not make them look bad.

1 MS. CHARLESWORTH: Okay. Now Professor
2 Matwyshyn and Professor Bellovin.

3 MS. MATWYSHYN: Just a brief comment on
4 the point of the cars that was raised.

5 So, indeed, car companies such as Tesla
6 are implementing the state-of-the-art security
7 processes in place. However, there's
8 unfortunately a large degree of variation in
9 security processes across car manufacturers.

10 And because, for example, some car
11 manufacturers have not yet fully staffed out their
12 security teams and have a large number of job
13 openings for security personnel, for example, on
14 their websites, it would certainly be beneficial
15 for them to engage with the security community
16 more aggressively.

17 And Tesla, for example, is on the face
18 of things, ISO-compliant. They have not opposed
19 our approach. And, in fact, they are bringing a
20 car to DEF CON, one of the major computer security
21 conferences, and asking participants to engage
22 with the car and to find flaws in the car. That
23 is the best practice for security in the auto
24 industry.

25 And if every car company was on the

1 level of Tesla, we would not be concerned about
2 that industry in particular. And the security
3 researchers are very concerned about that industry
4 in particular.

5 MS. CHARLESWORTH: Professor Bellovin?

6 MR. BELLOVIN: One of the issues with
7 notification -- and I certainly am in favor of
8 notification. I have done it myself in the times
9 I have found vulnerabilities -- is whether or not
10 the vendor would have the legal right to block or
11 delay publication. This actually interacts in a
12 bad way with university policies.

13 I may not accept a grant, for example --
14 this is university policy, not personal policy. I
15 may not accept a grant that gives the funding
16 agency or some outside party the right to block
17 publication. The university sees this as a very
18 fundamental matter of academic freedom that nobody
19 else do it. And it's university policy.

20 And it's actually mirrored in an odd
21 place in the law having to do with the export laws
22 on technology. What is export? There's something
23 called "deemed export." You cannot teach foreign
24 nationals certain things under certain conditions.
25 That's in technologies, including perhaps

1 encryption.

2 But one of the things that it says in
3 the law last time I looked -- and this was about
4 eight years ago -- was that fundamental research
5 is okay, but -- and what defines fundamental
6 research? One of the criteria is: Can somebody
7 else block publication?

8 If someone else can block publication,
9 than it is not considered fundamental and the
10 export control rules can't apply, which causes
11 other very serious chilling effects for academics,
12 including criminal sanctions for violating these
13 export control laws, which are a very major
14 concern in the country today. Mostly not on this
15 grey area, but it is, indeed, a concern.

16 So the university is very careful to
17 avoid anything that lets somebody else block
18 publication. I cannot do grant-funded research
19 that, with a contract, gives somebody else the
20 right, precisely to preserve academic freedom and
21 also to protect me and my students under the
22 export laws.

23 MS. CHARLESWORTH: Professor Blaze?

24 MR. BLAZE: I'm sorry. I'm losing my
25 voice a little bit.

1 The -- I wanted to give an example along
2 the lines that Professor Bellovin was discussing.

3 In 2007, when I did research into
4 vulnerabilities in electronic voting systems --
5 which were the systems used to conduct
6 national elections throughout our country and
7 were clearly a very critical thing --
8 we very specifically, -- we, first of
9 all, found sweeping vulnerabilities across every
10 system that was tested that could be exploited to
11 affect the outcome of an election by somebody who
12 had fairly limited access.

13 MS. CHARLESWORTH: Sorry. That was
14 authorized research, right?

15 MR. BLAZE: It was not authorized by the
16 vendors, but it was authorized by the -- by
17 customers, the state governments that had approved
18 them. The voting machine vendors were not --
19 didn't -- didn't contract with us to do this but
20 rather the users of the voting machines contracted
21 with us.

22 MS. CHARLESWORTH: And did the vendors
23 ever pursue you at all over that?

24 MR. BLAZE: Well, we had a certain
25 shield over us. We were indemnified under state

1 law, and there was some contractual back-and-forth
2 with the voting machine vendors that I wasn't
3 myself privy to that allowed the state governments
4 to indemnify us.

5 So it falls into a bit of a grey area
6 there.

7 But we -- one of the issues we addressed
8 was the question of whether we would give the
9 voting machine vendors advance notice to allow
10 them to fix it. And we, in this particular
11 example -- although we normally do try to give --
12 in my community, ordinarily will try to give
13 notice to the -- to the vendors.

14 In this case, we felt that allowing the
15 end users to remediate immediately through
16 procedural changes that we would -- that we
17 recommended outweighed the benefits of not
18 notifying the users and allowing the vendors more
19 time to repair things that would actually take
20 them longer than the next election to fix.

21 MS. CHARLESWORTH: So let me just -- I
22 just want to understand.

23 So did you notify the state authorities
24 so they could --

25 MR. BLAZE: So the state authorities --

1 MS. CHARLESWORTH: -- do a workaround?

2 MR. BLAZE: So the reports were
3 published. The state authorities were notified,
4 and the vendors were notified all simultaneously.

5 MS. CHARLESWORTH: Right. But the
6 vendors knew you were doing the research
7 generally?

8 MR. BLAZE: The vendors were aware that
9 we were doing the research but didn't see our
10 results until they were made public.

11 MS. CHARLESWORTH: Okay.

12 Ms. Moy?

13 MS. MOY: Yes. Thanks.

14 I just wanted to chime in quickly and
15 just emphasize again the importance of disclosing
16 not only so that the vulnerability can be remedied
17 but so that consumers who are in the market for a
18 product of the nature of the product that has a
19 vulnerability can make an informed decision about
20 which product is best for them.

21 If a -- if a vendor can stall
22 publication of the vulnerability for six months or
23 a year while it addresses that vulnerability but
24 continue to market the product in the meantime
25 without patching that vulnerability, I think that

1 that's an enormous problem and one that -- and one
2 that has major implications for consumers who are
3 in the market who deserve to know about that.

4 MS. CHARLESWORTH: Can I ask you a
5 question?

6 MS. MOY: Mm-hmm.

7 MS. CHARLESWORTH: Could some of that --
8 the need for consumers to know be addressed by
9 sort of a high-level communication that this has a
10 security problem without getting into the details
11 of how you would, you know, hack the system to do
12 something bad with it?

13 MS. MOY: I'm sure that that would
14 probably address the problem for some consumers. I
15 would say not all.

16 I mean, there are certainly going to be
17 cases where the nature of the vulnerability is an
18 important consideration. I mean, it would be
19 difficult to know without looking at it on a case-
20 by-case basis. But just talking about, you know,
21 the -- for example, the BMW vulnerability that was
22 -- that was publicized in January of this year
23 that was a vulnerability with the remote unlocking
24 -- with the remote unlocking function.

25 I think that there are details there

1 that might be important to certain consumers. Some
2 of the public reports that I read said that it
3 couldn't be used -- that vulnerability couldn't be
4 exploited to unlock other people's cars; it could
5 only be exploited to unlock your own. I don't
6 know if that's true. I don't know if that's the
7 case.

8 But, you know, I'm sure that there are
9 consumers who would read reports like that and
10 make a decision for themselves about whether or not
11 they're willing to take on the risk of purchasing
12 a product with that known vulnerability addressed.

13 MS. CHARLESWORTH: But the report -- I
14 mean, in that, you're saying there's some detail,
15 there's some information --

16 MS. MOY: Mm-hmm.

17 MS. CHARLESWORTH: -- about what it is.
18 Obviously it isn't step-by-step instructions on
19 how to hack the BMW system; is that correct?

20 In other words, why would your -- why
21 would an ordinary consumer need to know that?

22 MS. MOY: Well, I mean, ordinary
23 consumers include people who have -- who have an
24 understanding of how the technology works. Right?

25 I mean, we -- yeah, many consumers --

1 for example, myself, I would not be able to know
2 even by reading a technical explaining of how --
3 of how the vulnerability can be exploited, I
4 wouldn't be able to do it.

5 But someone like Professor Green or
6 Professor Bellovin would understand, and that
7 information might be important to them and to
8 others that -- you know, to others like them, also
9 to others who might read materials that they would
10 write on the subject.

11 MS. CHARLESWORTH: But what I'm trying
12 to get at is, as Mr. Troncoso's concern, right,
13 that by publishing the detail of how to exploit a
14 vulnerability, you are enabling that -- the claim
15 is you're enabling a certain group of people who
16 might not otherwise have known about it or done
17 that to do it -- bad guys. Not really
18 sophisticated ones who are out there all the time
19 but the kind of -- you know, and that -- but to
20 know -- to warn consumers, you don't need -- I
21 mean, I would think in the ordinary case, you
22 could concede that a consumer, you know, who says,
23 "Oh, my gosh. There is a problem with the BMW,"
24 then is on notice and can take additional steps,
25 if they want, to find out more about it or -- you

1 know, or at least talk to BMW about it.

2 But in the ordinary course, why would
3 you need to have step-by-step instructions on how
4 to exploit the vulnerability? And why would that
5 even be a good thing?

6 MS. MOY: Well, part of what I'm saying
7 also, though, is that the -- the detailed
8 description of what the vulnerability is would be
9 important to provide information to those who can
10 translate what the -- the nature of the
11 vulnerability and the severity of the risk to
12 everyday consumers as well.

13 MS. CHARLESWORTH: But -- I mean, you're
14 -- I'm really struggling with this.

15 MS. MOY: Mm-hmm.

16 MS. CHARLESWORTH: If I were buying a
17 car -- I'm like you. I'm not someone who's that
18 sophisticated -- and someone
19 said this -- let's take the pig example --
20 "This pig allows people to intercept
21 communications with your child," and then I can
22 decide whether I want to take it back to Toys"R"Us
23 and demand a refund. I can decide -- I mean, why
24 do I need to know this specific
25 as your typical consumer -- typical

1 consumer, why do I need to know the specific
2 reason or way that you exploit that system? I
3 mean, why -- why does that need to --

4 MS. MOY: But let me respond --
5 to that with another question and
6 say: How is it that you know at that
7 high level who's going to translate the -- who's
8 going to translate the nature of the vulnerability
9 for the -- for the consumer?

10 MS. CHARLESWORTH: Okay. Mr. Stanislav
11 is going to write an article, and he's going to
12 say, you know, "I tried to" -- you know, I don't
13 know the -- all the -- you've mentioned the
14 scenario.

15 But I mean, the company, let's say,
16 refuses to fix it. And for whatever reasons, he
17 decides to publish an article or to alert news
18 outlets and says, "This toy has a big problem. It
19 allows people potentially to hack in and intercept
20 communications with your child, and you should get
21 the word out there because people should be
22 informed consumers and should know that if they're
23 buying this toy."

24 That's how I would know. I wouldn't
25 need to know the specific line-by-line

1 instructions on how to hack into the system or the
2 toy in order to make a decision whether I wanted
3 my child to continue to have that toy.

4 MS. MOY: So isn't --

5 MS. CHARLESWORTH: And I --

6 MS. MOY: Sorry.

7 MS. CHARLESWORTH: I mean, can you --
8 can you concede that?

9 MS. MOY: I mean, I --

10 MS. CHARLESWORTH: Why is that so hard
11 to concede?

12 MS. MOY: It's -- well, the -- I -- as I
13 said, I think that that would -- that would
14 satisfy it for a lot of consumers. I think that
15 there are still some for whom that would not be
16 sufficient information.

17 I also --

18 MS. CHARLESWORTH: Why?

19 MS. MOY: -- am having a --

20 MS. CHARLESWORTH: Why?

21 MS. MOY: -- hard time envisioning --
22 sorry. I'm just -- I'm also having --

23 MR. STANISLAV: I can address that if
24 you want. I have an answer for that.

25 MS. CHARLESWORTH: Okay. Well, I want

1 to -- I want to have Ms. Moy explain why, and then
2 -- and then you can address that.

3 MS. MOY: Well, the problem is that I am
4 not a consumer like Mr. Stanislav. Right? I
5 mean, the -- I can tell you that that would be
6 sufficient for me, but I can tell you that I think
7 that it would be insufficient for other consumers
8 who are at a different level of sophistication
9 than I am.

10 In addition, I'm having a difficult time
11 from a legal perspective envisioning what -- how
12 you would cabin an exemption in such a way that
13 there were disclosure allowed but not with the
14 particular level of technical detail that would
15 facilitate replication of the vulnerability and --
16 I mean, which I think is another -- that is --
17 that is also at the heart of the problem here.
18 Right? I mean, what we're
19 describing is maybe a legal distinction
20 that I think would be very difficult
21 to put into an actual exemption.

22 MS. CHARLESWORTH: Well, I mean, I think
23 Congress was driving at this a little bit in (j).
24 And it says it's solely to promote the security of
25 the owner or operator of the computer or computer

1 system or computer network and shared directly --
2 I mean, in other words, I think part of the policy
3 that I'm seeing in there was the idea that you
4 weren't necessarily advising the world how to do
5 this, but it was -- you were doing the research in
6 a way that didn't enable malicious actors.

7 I mean, I -- you know, it's not stated
8 expressly, but that's -- again, that's what

9 Congress -- Congress here looked at --
10 we're all -- we're hearing the same thing: This
11 is complicated. There's a lot of -- Congress kind
12 of put this test in here and one of the
13 factors, I think, is sort of looking at whether
14 you use the research responsibly and whether it
15 was disclosed responsibly and so forth.

16 So I think you can -- you could -- I
17 could write a law that did that. I could

18

19 MS. MOY: Yeah. I mean, I also --

20 MS. CHARLESWORTH: -- but --

21 MS. MOY: I also -- as a consumer, I
22 would want to -- I would also want to read others'
23 analysis of how bad the vulnerability is and also
24 -- not only how bad is the vulnerability -- is the
25 specific vulnerability but what are the

1 implications for the way that this company
2 approaches security. Right?

3 I mean, is it a vulnerability that a
4 company -- even a company implementing reasonable
5 security practices could have built into a system
6 and -- or is it something that represents a major
7 oversight? And I -- I would want to know the -- I
8 would want to see the analysis of parties that I
9 trust who are capable of translating the technical
10 details into a -- into a report, perhaps a
11 journalistic report or an academic report, that I
12 can read as a consumer and determine for myself
13 whether or not I'm willing to take on that risk
14 and whether or not I'm willing to trust the
15 company to address security concerns sufficiently
16 in the future.

17 MS. CHARLESWORTH: I mean, do you think
18 a high-level disclosure is better than no
19 disclosure? In other words, a high-level one that
20 didn't have the specific instructions in terms of
21 how to exploit the vulnerability versus no
22 disclosure?

23 MS. MOY: I mean, if those are the
24 options that consumers are given, then yes. I
25 think more information for consumers in the

1 marketplace is generally a good thing.

2 But, again, I don't think that that
3 would -- I don't think that that would get to all
4 of the reasons that we want to see disclosure of
5 vulnerabilities.

6 MS. CHARLESWORTH: Okay. Thank you, Ms.
7 Moy.

8 I think, Mr. Stanislav, you had a
9 specific response.

10 Then we'll -- then we'll circle around
11 the room again.

12 MR. STANISLAV: Yeah, very briefly.

13 So two things. One being: I pulled up
14 an article at the time of the research in Exhibit
15 12 of the web camera. The CTO at the time was
16 quoted as saying that my research was inaccurate
17 and misleading -- and had misleading information.
18 I've since presented the research on this publicly
19 at many security conferences and also software
20 engineering conferences. I have the proof to back
21 it up.

22 And so when a story like this comes out
23 and the vendor says that I am lying, I have the
24 proof to show consumers what their actual risks
25 are.

1 The second part of that is prevention.
2 Whether it's a firewall manufacturer, a router
3 manufacturer, an anti-virus company, if they do
4 not know the specific details of the
5 vulnerability, they cannot protect the consumer in
6 the meantime until the vendor gets a release patch
7 out, whether it's five days or five years or
8 never.

9 MS. CHARLESWORTH: Okay. Thank you, Mr.
10 Stanislav.

11 MR. STANISLAV: Thank you.

12 MS. CHARLESWORTH: Mr. Sayler?

13 MR. SAYLER: So just building on this a
14 little bit. I mean, if we go back to the example
15 of the blog post Mr. Stanislav writes with the
16 high-level disclosure, you know, targeted at
17 consumers, I mean, I would argue that the
18 technical disclosure is hugely important.

19 And it's not necessarily for the
20 individual consumers; it's for people like me that
21 are now going to go read that blog post and go,
22 "Well, this toy is maybe not unique. It's using a
23 microchip that other people have probably bought,
24 and this issue may exist in a wide range of toys.
25 I'm going to go out to Toys"R"Us. I'm going to

1 buy myself, you know, 20 toys. And I'm going to
2 replicate what he did on all of them to see where
3 else this vulnerability may exist so that I can
4 then disclose those to those manufacturers and to
5 those consumers."

6 I mean, the ability to duplicate and
7 replicate research is hugely important. And maybe
8 not to the average consumer, but it requires
9 public disclosure in order for those of us in the
10 community who do that kind of work to replicate
11 and undertake those kind of -- those kind of
12 efforts.

13 Getting back to Mr. Troncoso's point a
14 little bit about not wanting to increase the
15 number of zero days. So, you know, zero day being
16 a bug that no one knows about yet and thus that an
17 adversary can potentially exploit before someone
18 has a chance to patch it.

19 He mentioned the black markets where
20 exploits are traded, and that is an unfortunate
21 reality of the world. And I think, unfortunately,
22 many of the flaws that security researchers
23 discover might very well already be available on
24 the black market. Right? We're not necessarily
25 the first to discover it. We're just the first to

1 discover them and tell the world about them.

2 You know, if I had a half a million
3 dollars and I wanted to go buy one of these, I
4 might be able to do it already. So I don't
5 necessarily think we're increasing the number of
6 zero days by allowing certain forms of public
7 disclosure. I think it's more an issue of the bad
8 guys may very well already know about a lot of
9 these, and the disclosure allows the good guys to
10 find out about them and see how bad they actually
11 are.

12 MS. CHARLESWORTH: Well, that's the
13 argument. And the argument on the other side is:
14 There's a certain number of them that people may
15 not know about, and you'll be educating them.
16 That's the concern.

17 MR. SAYLER: Yeah. And, I mean, then
18 there's a balance here. Right? The question
19 becomes: Is it okay to maybe have some people who
20 are going to find out about this via your public
21 disclosure, but in response you're going to
22 protect millions of end users who now know there's
23 a piece of software they should no longer use?

24 I mean, this gets at the very
25 complexities of this whole disclosure question,

1 and I think the reason for some of our pushback on
2 this is it is so complex and it's extraordinarily
3 hard to codify in a specific written exemption how
4 to do this properly.

5 And to some extent -- I mean, yeah,
6 maybe we are saying it would be great if we could
7 just rely on individual security researchers, you
8 know, practicing good faith -- whatever that means
9 -- research, that they will do this properly. And
10 I guess I don't have a great response for, you
11 know, what happens when they don't.

12 But I think the benefits of allowing
13 them that latitude far outweigh the downsides that
14 the adversaries might use by exploiting these kind
15 of exemptions.

16 MS. CHARLESWORTH: Okay. Let's see. We
17 have -- okay -- a few more minutes.

18 I want to go -- I'm going to start --
19 I'm going to go around this way because Mr.
20 Lightsey's had his placard up. But I will get to
21 everyone.

22 This will be kind of, I think, the last
23 round of comments that we'll have time for.

24 Mr. Lightsey?

25 MR. LIGHTSEY: Yeah, just very briefly,

1 just to protect the record. I will say that, on
2 behalf of GM, cybersecurity is certainly something
3 that we take very seriously. And we have an
4 extensive organization under a senior leader at GM
5 who's responsible for that.

6 As I indicated in California, it's a
7 subject that's reported quarterly to our board of
8 directors. This certainly has the highest
9 attention of GM management.

10 On behalf of the industry, I can say
11 that the industry has committed to a set of
12 privacy principles voluntarily. One of the those
13 principles commits to maintain reasonable security
14 to protect people's information.

15 And as indicated, you know, that's
16 certainly something we understand is enforceable
17 under Section 5 of the FTC.

18 And then, finally, we are also engaged
19 in putting together a cyberthreat sharing
20 organization where the entire industry will
21 participate and share cyberthreat information.

22 Thank you.

23 MS. CHARLESWORTH: Thank you.

24 Mr. Troncoso?

25 MR. TRONCOSO: I just wanted to make a

1 couple of points. Earlier the issue was raised
2 about the potential for software companies to just
3 decide we're not going to fix a problem that
4 you've notified us about.

5 But I would just sort of point to the
6 fact that we do have regulators in place to handle
7 situations exactly like this. So if security
8 researchers are encountering pushback from
9 software companies who are just outright unwilling
10 to fix problems that they've been notified about,
11 I would urge them to go to the FTC, for instance,
12 and have the issue resolved that way.

13 And then sort of circling back now to
14 the zero-day issue --

15 MS. CHARLESWORTH: Can I -- can you
16 pause for a moment?

17 MR. TRONCOSO: Yeah.

18 MS. CHARLESWORTH: What would the -- I
19 mean, tell me more about the FTC process.

20 MR. TRONCOSO: Laura -- Ms. Moy brought
21 this up in her testimony. She indicated that the
22 FTC has been willing to prosecute -- or not
23 prosecute -- but to bring enforcement actions
24 against companies who are not employing sufficient
25 safety standards in their products and that

1 they've done so in this specific space of security
2 vulnerabilities.

3 So I think that that's sort of where I
4 was going with that. I don't have more specific
5 information than what was presented, though.

6 On the second issue of the zero-day
7 vulnerability concerns, I think that building in a
8 requirement to disclose vulnerabilities to the
9 vendor of the software is critical to ensuring
10 that there are not perverse incentives for
11 researchers to keep their research hidden so that
12 it's more valuable on the grey and black markets.

13 Of course, we're not talking about the
14 researchers in this room, of course. We're
15 talking about the potential for this exemption to
16 be exploited by researchers who are not in this
17 room, who are the sort of bad actors that we have
18 concerns about.

19 MS. CHARLESWORTH: Thank you.

20 Let's see. Yes.

21 MR. STALLMAN: I'll be quite brief. Just
22 to respond to that issue, I don't know that we
23 have great visibility into the -- into the black
24 and grey markets for security exploits, but I
25 think it definitely is the case that part of the

1 value of the exploits that are trafficked in is
2 their secrecy, is the fact that they are -- they
3 are unknown.

4 And so publication, I think, is one way
5 to quickly make what might be a previously
6 existing but unknown to the -- to the broader
7 research community vulnerability swiftly lose its
8 value as something that should be trafficked in
9 the black market.

10 So I think that's a reason to encourage
11 more disclosure and more -- sorry -- more
12 publication and disclosure.

13 MS. CHARLESWORTH: Thank you, Mr.
14 Stallman.

15 Professor Blaze?

16 MR. BLAZE: So thank you. I'll be very
17 brief.

18 So two points. First of all,
19 there is a bright-line difference
20 between the legitimate scientific research
21 community and the black-market criminals, which is
22 that we publish our work and we're required to
23 publish our work because that's what the
24 scientific method demands.

25 So this -- you know, disclosure is

1 simply -- public disclosure is simply part of our
2 process.

3 You asked about a compromise type of
4 disclosure to the public in which you describe the
5 existence of a vulnerability without describing
6 how to exploit that. And I -- when I think about
7 how I would implement that, I can think of some
8 examples in which it might be possible to tell
9 somebody that here's how
10 you can tell that you're
11 vulnerable. Here's what you can do to remediate
12 the vulnerability without giving you enough detail
13 to exploit it.

14 But I can think of many, many others in
15 which that would be sufficient information to
16 trivially derive what the details are, that the
17 existence and the way of telling whether or not it
18 applies to you is tantamount to
19 revealing how to -- how to exploit it.

20 So I'm not sure that a meaningful line
21 can be drawn there unless -- and I think the
22 people on that side of the table would agree --
23 unless we ask people to make very, very broad
24 statements like, you know, "Well, there's a
25 terrible life-threatening problem with GM cars,

1 and I can't tell you what it is." You know, I
2 think -- you know, being able to say, "This model
3 GM car has this type of problem with the brakes"
4 is much more valuable to everybody concerned.

5 MS. CHARLESWORTH: Right. But, I mean,
6 what I'm driving at -- and, you know, it's --
7 saying something has a problem with the brakes,
8 the software isn't performing correctly, you know,
9 is different from saying, "There's a vulnerability
10 here. And here's how you exploit it" and line-by-
11 line instructions.

12 I mean, do you -- don't you ever make
13 those distinctions in your writing?

14 MR. BLAZE: Sure. And sometimes it's
15 possible --

16 MS. CHARLESWORTH: I mean --

17 MR. BLAZE: -- you know, and I'm
18 certainly not going to suggest that it's never
19 possible to do that. In some cases, the technical
20 details for exploiting it are much -- involve
21 very, very specific things.

22 But in other cases -- in other cases,
23 they aren't. So, for example -- and, you know,
24 I'm speaking totally hypothetically here. I don't
25 actually own a car, let alone a GM car.

1 You know, it may be that there are many
2 models of cars, some of them are vulnerable, some
3 of them aren't. And the vulnerability is that, if
4 you turn the turn signal to the left three times,
5 it causes the brakes to stop working. And that's
6 -- you know, and the only way to tell whether the
7 car that you've got has that vulnerability is to
8 try it. And there's no other way to describe this
9 vulnerability except with information
10 that's tantamount.

11 And it's going to vary across the
12 spectrum from that to cases where you could
13 obscure it. And I don't think we can draw a
14 generally applicable line that would meaningfully
15 separate the two.

16 MS. CHARLESWORTH: Okay. But just to --
17 just a quick question. I mean, when you publish
18 your research --

19 MR. BLAZE: Mm-hmm.

20 MS. CHARLESWORTH: -- I assume in some
21 situations, I mean, you refrain from giving
22 detailed information. I mean, does that ever
23 happen -- about how to hack a system because you
24 think maybe it actually might be harmful?

25 MR. BLAZE: Absolutely. And it depends

1 on -- and really the test is whether or not, in
2 order to explain what the vulnerability is and in
3 order to explain what the problem is so that
4 others can learn from it and so that people can
5 protect themselves against it, you know, is it
6 necessary to include details that will allow its
7 exploitation?

8 And sometimes the answer is: Well, the
9 exploitation involves doing a lot of very, very
10 specific, detailed steps that are -- you know,
11 that aren't essential to understanding it. But in
12 other cases, everything essential to understand it
13 gives you enough information to exploit it. And
14 then in still other cases, we're somewhere in the
15 middle where, you know, you're doing 90 percent of
16 the engineering of the exploitation and leaving 10
17 percent out. But a determined person could figure
18 it out.

19 And it's going to vary across that whole
20 spectrum.

21 MS. CHARLESWORTH: And when you say
22 that's -- the test is -- I mean, do you think
23 that's a widely shared view in the academic
24 security community? Or is that a generally held --

25 MR. BLAZE: I think --

1 MS. CHARLESWORTH: -- view?

2 MR. BLAZE: Sure. And with
3 the understanding that essential
4 property of the scientific process is
5 we publish papers that are reproducible that
6 others can test and that others can -- and that
7 others can build upon.

8 So we also have that
9 other demand on us that the readers of the
10 scientific papers that I write need to be able to
11 reproduce and verify my work.

12 But even separate from that, I think the
13 test of unnecessarily providing aid and
14 comfort to people who would do this for no good is
15 not something that any of us want to do.

16 MS. CHARLESWORTH: Okay. Thank you,
17 Professor.

18 Professor Matwyshyn?

19 MS. MATWYSHYN: Thank you.

20 Just to follow up, there's a whole array
21 of mitigation measures that the researchers can
22 talk with us about, that researchers regularly
23 engage in in the course of their disclosure
24 processes already.

25 Sometimes it's leaving out essential

1 detail. Sometimes it's changing the timing of a
2 disclosure. But there's a bundle of tools that
3 researchers use currently as best practices, as
4 norms within their own self-governance in the way
5 that they engage with and disclose.

6 MS. CHARLESWORTH: Are those written
7 down anywhere? Or is it just sort of in the air?

8 MS. MATWYSHYN: It is -- well, the
9 researchers are better positioned to talk about
10 this. But in general, they are in there because
11 they are contingent upon the nature of the
12 reproducibility.

13 MS. CHARLESWORTH: So there are no
14 written -- are there any? I mean, are there any
15 written best practices?

16 MS. MATWYSHYN: The closest are the ISO
17 standards.

18 MS. CHARLESWORTH: Which really -- okay.
19 Thank you.

20 MS. MATWYSHYN: So two more quick
21 points. On the point of the zero-day vulnerability
22 markets and markets in vulnerabilities generally,
23 from the researcher perspective, the researcher
24 faces a decision. That's why this proceeding is
25 so important.

1 The researcher is in possession of
2 knowledge of a vulnerability. That researcher
3 gets to choose at present: Do I sell this
4 vulnerability and make a quick buck and wash my
5 hands of it; or do I undertake the laborious and
6 personally risky process of attempting to contact
7 vendors, have them potentially threaten me with
8 the DMCA, engage in months of conversations trying
9 to convince people there is a problem when they
10 might not believe me, and then --

11 MS. CHARLESWORTH: Are you saying
12 there's an overlap in those communities, the
13 people who would --

14 MS. MATWYSHYN: There's a choice.

15 MS. CHARLESWORTH: There's a choice.
16 But, I mean, aren't we talking about good-faith
17 people here who would not be selling --

18 MS. MATWYSHYN: But -- so -- but in the
19 grey areas, the --

20 MS. CHARLESWORTH: But --

21 MS. MATWYSHYN: So the market in zero
22 days is not currently criminal, and the U.S.
23 government in particular purchases zero
24 days regularly.

25 So researchers frequently feel that they

1 have a choice with these most elite
2 vulnerabilities. But the majority of
3 vulnerabilities are not that sophisticated.
4 They're commonly known vulnerabilities that have
5 simply not been patched.

6 And so frequently a discovery will
7 happen when a researcher is using a product and
8 noticed that this product has not patched this
9 ten-year-old vulnerability that has been widely
10 known for a long time. And then we want those
11 researchers to contact the company, and we don't
12 want something like the DMCA to prevent the
13 researcher from doing this act of public service
14 and assisting the company in correcting this flaw.

15 And, finally, on the point of the FTC, I
16 served as the FTC senior policy adviser on privacy
17 and security last year. So the way that the FTC
18 engages with security -- it performs an incredibly
19 valuable function, but it is an agency with
20 limited resources. And so although it has engaged
21 in over 50 enforcement actions on security and
22 reasonable security standard implementation by
23 companies, there hasn't a formal intake mechanism
24 for consumers to report problems other than
25 consumer sentinel or for security researchers to

1 report problems through a trusted type of hotline.

2 Such a hotline for security researchers
3 does not currently exist at the FTC, and the FTC
4 cannot act as the mediating vector for DMCA
5 threats from vendors. And so the FTC's role is not
6 quite apposite here with respect to our DMCA
7 questions.

8 MS. CHARLESWORTH: Well, okay. I mean,
9 you said something that was somewhat disturbing to
10 me, and I -- I questioned you a little bit. But I
11 mean -- and maybe this is sort of a side
12 conversation.

13 But you're suggesting that the people
14 we're trying to grant the exemption to -- or who
15 would benefit from this exemption, if they don't
16 get it, could -- might sell research on the black
17 market? I mean, I hope I misunderstood that.

18 MS. MATWYSHYN: So there is a -- this is
19 -- the zero-day market is a very small sliver of
20 what we're talking about here.

21 MS. CHARLESWORTH: But is it --

22 MS. MATWYSHYN: A very small sliver.

23 MS. CHARLESWORTH: How does it play into
24 this? I mean, you're --

25 MS. MATWYSHYN: A zero-day vulnerability

1 is one type of flaw that can exist.

2 MS. CHARLESWORTH: No, I understand --

3 MS. MATWYSHYN: And so in the absence of
4 a regulatory regime for zero-day vulnerabilities
5 broadly, which we don't currently have --

6 MS. CHARLESWORTH: But we have 1201,
7 which says you can't -- you can't circumvent -- I
8 mean, in other words, you're assuming someone has
9 discovered a zero-day vulnerability.

10 MS. MATWYSHYN: Right.

11 MS. CHARLESWORTH: With circumvention or
12 without? I mean, have they already broken the law
13 or have they not? I mean --

14 MS. MATWYSHYN: If in the course of the
15 discovery of the vulnerability they may have
16 circumvented, we want them to report it to the
17 company and to the public.

18 MS. CHARLESWORTH: Right.

19 MS. MATWYSHYN: We want to encourage --

20 MS. CHARLESWORTH: But if they've
21 already circumvented in violation of 1201, why do
22 they care -- I mean -- I guess, why would --

23 MS. MATWYSHYN: So the act of disclosure
24 exposes a researcher to risk.

25 MS. CHARLESWORTH: So you're saying that

1 the -- those -- there are researchers that --
2 you're asserting that there are researchers who,
3 without this exemption, will take their research
4 and sell it on the black market?

5 MS. MATWYSHYN: We don't want that to
6 happen.

7 MS. CHARLESWORTH: We don't, but --

8 MS. MATWYSHYN: We want to nudge
9 everyone toward disclosure.

10 MS. CHARLESWORTH: But do you have any
11 evidence that that has actually happened, that
12 people who -- I mean, it's just a -- it's a
13 disturbing -- it's kind of a disturbing argument
14 here.

15 MR. BELLOVIN: Well, I don't know if --
16 I don't know enough of the facts to say if it was
17 a choice. But Charlie Miller, who's one of the
18 foremost researchers to automotive vulnerabilities
19 -- he's an ex-NSA hacker, from his own
20 description, and has stated in interviews that he
21 has found a vulnerability of sufficient interest
22 to some unnamed U.S. government agency, that he
23 sold it for some unspecified but high-five figures
24 value to the U.S. government.

25 So here's someone who is finding and

1 publishing vulnerabilities who's also sold an
2 interesting vulnerability to some part of the U.S.
3 intelligence community.

4 I don't know any more details than that
5 and, of course, he's not going to say.

6 MS. CHARLESWORTH: Professor Bellovin --
7 well, both -- Professor Matwyshyn, I think you
8 finished your final comments there.

9 Professor Bellovin, did you have
10 anything else to add?

11 MR. BELLOVIN: I would add I served as
12 chief technologist to the Federal Trade Commission
13 for a year, and I will second what she said: It
14 does not have the resources to act as an
15 intermediary in most of these cases.

16 In particular, it is not a consumer
17 protection agency in the case of resolving
18 individual cases of a bogus DMCA takedown threat,
19 for example, or "Don't do this research." It's
20 not the purpose of the agency.

21 Most of what I was going to say was
22 already said by Professor Blaze.

23 I would say that security researchers,
24 from just very vague information, just disclosure
25 of the very vague information is enough to reveal

1 the really interesting parts.

2 So take automobiles. The automobile
3 hacking case that I'm most familiar with involved
4 vulnerabilities in the wireless tire pressure
5 monitoring system. You know, it never would have
6 occurred to me to go look into that.

7 Once I knew that there was an attack
8 there, it probably would have taken me only a few
9 weeks to recreate the work that -- for any
10 competent security researcher to recreate the work
11 once they were pointed in that direction.

12 "There's a security vulnerability in the
13 tire pressure monitor wireless system." That
14 statement alone is enough for the serious enemies
15 -- and those are the ones I'm most concerned about
16 -- to do it. You don't need the details at that
17 point. Asking the question -- the right question
18 is often the very hardest part of this kind of
19 research, and it's very hard to say -- you know,
20 should this vulnerability have said, you know,
21 "Get rid of it. It's dangerous"? Well, do the
22 batteries overheat if it's rechargeable batteries?
23 Do I worry about a three-year-old pulling this
24 off, or do I worry about a software flaw?

25 Different remediation measures for

1 consumers are indicated in each of those three.

2 When I hear there's a software flaw in
3 this, it would not take me long at all to find it,
4 to recreate it. Knowing to look there was the
5 hard part.

6 MS. CHARLESWORTH: Okay. Again,
7 referencing the famous Exhibit 12.

8 Okay. We're coming down to the wire
9 here.

10 Mr. Sayler, are you going to defer to
11 Professor Reid?

12 MR. REID: So I just wanted to chime in
13 and underscore Professor Bellovin's point about
14 remedies because I think it's not just about the
15 understanding -- although I think -- about
16 understanding the vulnerability and explaining the
17 vulnerability. It's about, in some circumstances,
18 consumers being able to take an actual remedial
19 action. And sometimes explaining that takes some
20 detail.

21 So we might look at Exhibit 12 and say,
22 "You know what? There's a piece of crappy
23 software in there, and you should just throw this
24 thing away if you own it because it's not worth
25 the trouble to fix it."

1 But if I say the same thing to you about
2 your car, you're going to say, "Well, wait a
3 minute. I paid a lot of money for my car, and I
4 can't just go throw my car away. Tell me more
5 about it. Tell me how it fix it."

6 And if you look at how the auto industry
7 handles other kinds of problems -- so I just
8 Googled, because I own a Honda Element, and we got
9 a recall notice about the air bag in it.

10 I just Googled it, and the first article
11 that came up is a 30-page article explaining every
12 detail about the vulnerability, every factory
13 where the vulnerable air bags came from,
14 everything that led to the air bags potentially
15 having a problem.

16 I can look up my VIN number. I can plug
17 it into a web page, and I can find out if my car
18 has a problem. I can schedule an appointment to
19 fix it.

20 And then I looked up similarly --

21 MS. CHARLESWORTH: Excuse me. Is that a
22 software vulnerability or --

23 MR. REID: No. I'm just trying to draw
24 an analogy to --

25 MS. CHARLESWORTH: Okay.

1 MR. REID: -- nonsoftware
2 vulnerabilities.

3 MS. CHARLESWORTH: But that's not a
4 software issue?

5 MR. REID: If I -- if I type in "can
6 hackers hack my car," which is -- if you start
7 typing "can hackers," the first thing that comes
8 up on Google is "control my car," all I get is a
9 scary "60 Minutes" video where somebody sitting in
10 the back, Lesley Stahl sitting in the front, and
11 her car is going all over the place and she's kind
12 of freaking out.

13 And it says, "What can I do about it?"
14 And it says, "For now, not much."

15 And I think the difference here, if you
16 want to look at it, is that we've got the DMCA in
17 one instance and not in the other. And
18 researchers need to be able to disclose more in a
19 lot of circumstances to explain to consumers
20 exactly what's going on here and to apply the
21 kinds of pressure that Ms. Moy talked about.

22 So I just wanted to underscore the point
23 of consumer remedies can be really important when
24 we're talking about the granularity of the
25 disclosure.

1 MS. CHARLESWORTH: Thank you, Professor.

2 And, Mr. Sayler, you have your sign up,

3 but you were done?

4 MR. SAYLER: Yeah.

5 MS. CHARLESWORTH: Okay. So I'm going

6 to just ask -- quickly poll my colleagues here to

7 see -- Mr. Ruwe has one more question.

8 MR. RUWE: Mr. Stanislav, what was the

9 name of your former employer, the one that you

10 worked for when you identified the concern

11 regarding the pig?

12 MR. STANISLAV: Duo Security.

13 MR. RUWE: And what were their primary

14 services?

15 MR. STANISLAV: Two-factor

16 authentication, security for authentication.

17 MR. RUWE: All right. Thanks.

18 MS. CHARLESWORTH: Okay. Ms. Smith?

19 MS. SMITH: Professor Matwyshyn, you

20 said that the norms of the community are perhaps

21 best written out in the ISO standards.

22 And, you know, something concerning me

23 today is there's a lot of talk about these norms

24 and respecting the norms, not to hack a plane when

25 it's moving; or in patients, not to test a medical

1 device that's already implanted into a patient.

2 Is there anything in the standards that,
3 you know -- or similar standards that has not been
4 shared with the office or that could -- or any
5 type of standards into what makes a security
6 researcher a security researcher?

7 MS. MATWYSHYN: So security researchers,
8 in the opinion of the community about themselves,
9 is driven by the nature of the conduct of the
10 individual. Someone who discloses flaws for the
11 purpose of improving the security of our society
12 and works to better the vulnerable systems that
13 currently put us all at risk, that is a security
14 researcher.

15 The ISO standards are a moving target.
16 They're evolving. The discussions continue. And
17 the two individuals who lead the process have
18 stated that they are happy to directly consider
19 any issues that the panel feels should be
20 discussed with the community participating in the
21 ISO standard and to attempt to contemplate those
22 issues in the next round of the iteration of the
23 two ISO standards that we reference in our
24 exemption request.

25 MS. SMITH: So do the ISO standards or

1 anywhere else have a definition of "security
2 researcher," like what you said? Did that come
3 from something?

4 MS. MATWYSHYN: So the ISO standards are
5 driven by the corporate end of addressing the
6 processes for security vulnerability intake, the
7 internal mechanisms, and the relationship with
8 researchers. So the ISO standards refer to that
9 side of the equation.

10 From the companies that are ISO-
11 compliant, I believe their perspective would be
12 that anyone who comes to them with a piece of
13 research that demonstrates an actual vulnerability
14 in their product is a security researcher for
15 their purposes. They have provided useful
16 information for improving the quality of the
17 product and the integrity of the code that is
18 embedded in the products that the company is
19 making.

20 And so when a company such as Facebook
21 or Google awards a bug bounty to someone who
22 brings this type of problem to the table, by
23 bringing that problem to the table and the problem
24 being replicated and being deemed genuine, that
25 triggers the award of the bug bounty and you are,

1 hence, a security researcher.

2 MS. SMITH: Because you brought it
3 forward?

4 MS. MATWYSHYN: Mm-hmm.

5 MS. CHARLESWORTH: I was just going to
6 ask: Why aren't those standards public?

7 MS. MATWYSHYN: The ISO standards?

8 MS. CHARLESWORTH: Mm-hmm.

9 MS. MATWYSHYN: So that is something
10 else that the two individuals chairing the
11 committees mentioned that they would affirmatively
12 raise and push for, to open up the standards and
13 to make them public.

14 But ISO is an organization that has
15 traditionally been closed. They issue standards
16 in a whole variety of corporate contexts, very
17 high credibility organization. And so
18 traditionally their standards have been closed,
19 but in this case, because of the tremendous social
20 value that would be implicated by an exemption
21 that, for example, relied on them, they are
22 amenable to requesting that the standards be
23 opened. And hopefully they will receive
24 permission from the organization.

25 MS. CHARLESWORTH: I mean, it's a little

1 -- I mean, if we were going to go down that route,
2 it's a little hard to draft a law that's based on
3 something no one can see.

4 MS. MATWYSHYN: Exactly. And so that's
5 why, in the last round of filing, we distilled the
6 main criteria that are embodied in those ISO
7 standards. And so that is an alternative framing
8 that addresses that closed system problem.

9 MS. CHARLESWORTH: Thank you.

10 MR. REID: Could I chime in very
11 quickly? And just to your point, I wanted to tie
12 back to something Mr. Troncoso said earlier, which
13 was something that a security researcher is not is
14 someone who's intending to invoke the exemption to
15 commit copyright infringement.

16 And I think, as we reflected in our
17 filing, we would be comfortable with a limitation
18 that makes clear that it's got to be for
19 noninfringing purposes. We think the statute is
20 expressly geared towards that.

21 And I think, to the extent you're
22 looking for a limitation that you could work in,
23 it's probably in all of the exemptions that you're
24 granting.

25 MS. CHARLESWORTH: Well, it's in the law

1 already. Right?

2 MR. REID: Right. We agree.

3 MS. SMITH: Or what was or not in
4 violation of any other applicable law, which is in
5 the current exemption?

6 MR. REID: I mean, just in the interest
7 of time, I'll defer to the discussion we had
8 earlier on that.

9 MS. CHARLESWORTH: Yes. I think, Mr.
10 Cheney, you were leaning forward. You're leaning
11 back now?

12 Okay. Well, I -- yes, Professor?

13 MS. MATWYSHYN: Just very quickly on the
14 last question. I think that that would
15 unfortunately be a suboptimal framing because many
16 of the problems that currently exist with respect
17 to chilling research suboptimally intertwines the
18 DMCA with other statutes which are problematized
19 in their own nature.

20 So, for example, the computer fraud and
21 abuse side has three circuits, what's on it. We
22 don't want this approach in addressing the
23 challenges that currently exist under the DMCA for
24 security researchers to fall victim to the flaws
25 of other regimes that aren't built into the

1 system.

2 MS. CHARLESWORTH: Okay. Can I just say
3 something?

4 We will not be granting an exemption
5 that somehow suggests that you can violate other
6 laws. I just -- I'm going to say that for the
7 record.

8 Professor Reid?

9 MR. REID: We're okay with that.

10 MS. CHARLESWORTH: Okay. Thank you.

11 Professor Bellovin?

12 MR. BELLOVIN: One last quick point. One
13 reason why there's not any strong formal consensus
14 on the vulnerability reporting mechanism is, well,
15 twofold.

16 One, as Professor Blaze said --
17 Professor Green said, it's often very hard to
18 understand how best to disclose something, so it's
19 always -- there are very often going to be grey
20 areas.

21 But the second and more germane one in
22 this context is a fear of vendors not acting in
23 good faith. Many -- as we have seen, there is a
24 chilling effect even when it does not seem to be a
25 copyright concern. There is a concern that many

1 vendors will act this way. Rightly or wrongly, we
2 have seen enough instances where no copyright
3 concerns have actually been implicated, but the
4 DMCA has been used as a club.

5 And that has led many people to reject
6 the notion of a consensus saying, "I will use my
7 best judgment, and I will not coordinate, not sign
8 onto a policy that gives somebody else the power
9 to act incorrectly."

10 MS. CHARLESWORTH: Okay. We've run
11 over. So I'm going to close this panel.

12 This was a very illuminating discussion,
13 and we really appreciate the strong turnout,
14 particularly from the academic community. It's
15 clear that you have deeply held feelings about
16 this, and it's a tricky issue. It's an important
17 issue. And we will -- I'm guessing we may well
18 issue some additional -- some specific questions
19 for you based on the discussion we had today. I'm
20 not sure exactly when that will be, but you will
21 have another opportunity to respond to those,
22 everyone here, before we come up with our
23 recommendation.

24 So thank you.

25 I think -- what time should we

1 reconvene? Let's see. 1:45...

2 I guess we -- I think people probably
3 can have -- there's a cafeteria right down the
4 hall. So I think we will try and get back on
5 schedule, 1:45, for panel -- for the panel on
6 unlocking, classes 11 to 12. See we'll see those
7 of you who are involved with that back here at
8 1:45.

9 (Whereupon, a short recess was held.)

10 MS. CHARLESWORTH: Welcome back to those
11 of you who were here before, and welcome to any
12 newcomers. This is the Sixth Triennial Rulemaking
13 Proceeding under Section 1201 of the Copyright
14 Act.

15 My name is Jacqueline Charlesworth. I'm
16 the General Counsel of the Copyright Office.

17 And I'm going to -- I'm going to go down
18 the line and have my colleagues introduce
19 themselves.

20 MS. CHOE: Hi. Michelle Choe at the
21 Copyright Office.

22 MS. SMITH: Regan Smith, Assistant
23 General Counsel.

24 MR. DAMLE: I'm Sy Damle. I'm Deputy
25 General Counsel.

1 MR. RUWE: Steve Ruwe, Assistant General
2 Counsel.

3 MR. RILEY: John Riley, Attorney-
4 Advisor.

5 MS. CHENEY: And I'm Stacy Cheney,
6 Senior Attorney at NTIA, U.S. Department of
7 Commerce.

8 MS. CHARLESWORTH: Okay. So you have --
9 are there more of us than you? I don't know.
10 Maybe it's a tie. Okay.

11 So as some of you may have heard from
12 earlier today, the point of the hearings is really
13 to kind of home in on the issues that are sort of
14 a little bit in dispute, maybe murky areas where
15 we have questions. And we do let everyone have a
16 brief opening statement.

17 But in making your remarks, I would
18 encourage you to focus on the issues where there
19 may not be full agreement or the law perhaps is
20 unclear.

21 We do frequently interrupt with
22 questions. So be prepared on that.

23 And, you know, we are familiar with your
24 written comments. So there's no need to sort of
25 review sort of your high-level comments if you've

1 already submitted them in writing because we did
2 carefully read them.

3 We try not to talk over one another.
4 Your remarks are being recorded by the court
5 reporter. And if you're -- I don't -- are there
6 any exhibits with this one?

7 So we don't have to worry about that.

8 If you want to add to the conversation,
9 tip your placard up, and we will get back to you
10 so that you can respond or add an additional
11 comment as you see fit.

12 And for the record, this is proposed
13 classes 11 and 12, unlocking wireless telephone
14 handsets and tablets.

15 So before we launch into the opening
16 statements, I'm told I'm going to have to -- this
17 is going to be very -- I'm going to go from right
18 to left in this one. I'm used to going from left
19 to right.

20 So we'll start with you -- I can't read
21 your name -- Mr. Mackey? No. To your left, who
22 is sitting next -- he's not a real person, or is
23 he -- no, he's -- are you going to be
24 participating on the record?

25 MR. MACKEY: Yes.

1 MS. CHARLESWORTH: Okay. What -- we'll
2 start with you. If you could just briefly give
3 your name and your affiliation or the interest you
4 have in the proceeding.

5 We'll go from right to left, and then
6 we'll start at your end and have you make your
7 opening remarks.

8 MR. MACKEY: All right. Good afternoon.
9 My name is Aaron Mackey. I'm with the Institute
10 for Public Representation at Georgetown University
11 Law Center. And I'm Of Counsel to Consumers Union
12 in their proposed exemption.

13 MS. CHARLESWORTH: Great. Thank you.

14 MR. SLOVER: I'm George Slover, Senior
15 Policy Counsel for Consumers Union.

16 MR. LAZARUS: Mike Lazarus, an attorney
17 for Telecommunications Law Professionals. And we
18 represent Competitive Carriers Association.

19 MR. HARRIS: Hi. Good afternoon. Eric
20 Harris with ISRI, the Institute of Scrap Recycling
21 Industries. And I'm Associate Counsel and
22 Director of Government and International Affairs.

23 MR. WEISSENBERG: Good afternoon. Brian
24 Weissenberg, a law student at Stanford Law School,
25 involved in the IP and Innovation Clinic there,

1 representing ISRI.

2 MS. LONG: Hi. I'm Donna Long. I'm
3 also a law student at the Stanford IP and
4 Innovation Clinic. And also with us here at the
5 table is Professor Phil Malone. He's the director
6 of the IP and Innovation Clinic, and he won't be
7 speaking today. He's just chaperoning us.

8

9

10

11 MS. CHARLESWORTH: Well, it's good to
12 know everyone is well chaperoned.

13 Hello, Professor Malone.

14 Okay. So, Mr. Slover, does that mean
15 you're kicking us off? Okay.

16 MR. SLOVER: Good afternoon. Consumers
17 Union, the advocacy arm of "Consumer Reports," is
18 pleased to be here to support our proposed
19 exemptions to allow consumers to unlock telephone
20 handsets and tablets so they can be connected to
21 other wireless networks and thereby extend their
22 useful lives, save money, and increase competition
23 and innovation.

24 We've introduced ourselves already, so
25 I'll skip that.

1 We note that no one filed an opposition
2 to our proposed exemption for tablets, and the one
3 party who filed an exemption in opposition to our
4 proposed exemption for handsets, TracFone, has now
5 joined with the Competitive Carriers Association
6 in support of a differently drawn exemption.

7 We're encouraged at the efforts to reach
8 a consensus.

9 Today I will talk about why we have
10 written the exemption the way we have identically
11 for handsets and tablets as they are functionally
12 equivalent for this purpose and why we think our
13 way is better than the other ways put forward.

14 We will also be happy to answer any
15 questions you might have for us.

16 But first I will briefly recount the
17 reasons why we believe these exemptions are
18 warranted, reasons that are more fully set forth
19 in our petition comments and reply comments.

20 To start with, this exemption has been
21 approved twice before in 2006 and 2010. And when
22 it was phased out in 2012, a public uproar led to
23 the President and Congress calling for its
24 restoration and the resulting bipartisan enactment
25 of legislation reinstating in and directing the

1 Copyright Office to consider expanding it to
2 include tablets.

3 The exemption we propose is modeled
4 closely on what Congress enacted last summer with
5 the expanse to tablets that Congress envisioned.

6 Second and perhaps more fundamentally,
7 mobile device unlocking has no business getting
8 caught up in the DMCA's prohibition on
9 circumvention, convenient as it may be for certain
10 wireless carrier business models.

11 As the Copyright Office has noted,
12 unlocking a mobile device has nothing to do with
13 copyright infringement in any meaningful sense.
14 Unlocking is about being able to use equipment the
15 consumer has legally purchased.

16 As we explain in our written
17 submissions, the focus for copyright analysis is
18 properly on the network-connecting software in
19 these devices. The locking software is important
20 only because it obstructs access to the
21 functioning software.

22 Even if the network-connecting software
23 is copyrightable, which is by no means clear, it
24 is not being copied in a copyright sense when the
25 device is connected to another network. It is

1 either being engaged or it is being bypassed. And
2 the only possible copying of the locking software
3 would be for the very limited purpose of getting
4 out of its way.

5 Any incidental copying or adaptation of
6 either locking or network-connecting software is
7 protected under Section 117 as an essential step
8 in making the phone or tablet function.

9 In the Unlocking Act, Congress removed
10 any issue regarding whether the owner of the
11 device also has to own the copy of the software to
12 get the protection of Section 117. Using the DMCA
13 to enforce the law prevents consumers from making
14 full legitimate use of the phone or tablet they've
15 purchased. It strikes at the heart of the
16 fundamental rights of ownership that have been a
17 cornerstone of our law for centuries.

18 It arbitrarily cuts short the useful
19 life of perfectly good devices, adds to
20 unnecessary waste, removes affordable alternatives
21 for cost-minded consumers, and props up anti-
22 competitive business models that restrict consumer
23 choices. It harms consumers on both the selling
24 and the buying side.

25 As we and others have established,

1 that's precisely what happened when there was no
2 exemption. And that, in a nutshell, is the harm we
3 are seeking to remedy.

4 MR. DAMLE: I just have -- I'm sorry to
5 interrupt you.

6 MR. SLOVER: Yes. Go ahead.

7 MR. DAMLE: I have a couple of
8 questions, but I'll start with one just to
9 establish for the record why you believe the
10 unlocking policies of the carriers are
11 insufficient for you.

12 MR. SLOVER: Well, you mean the
13 voluntary --

14 MR. DAMLE: Yeah, the voluntary
15 policies, right.

16 MR. SLOVER: Well, first of all, because
17 they are voluntary, which means they could be
18 changed at any time. So they're no substitute for
19 a right.

20 Secondly because there are restrictions
21 and conditions. You basically work through a
22 process with your current carrier to unlock the
23 phone. So that eliminates some of the flexibility
24 for consumers who would prefer not to deal with
25 their previous carrier, would rather turn over the

1 phone in a locked state and have somebody else do
2 the unlocking.

3 And, you know, because it can be
4 changed, you know, it's kind of -- over time, the
5 voluntary policies came to fruition when everybody
6 was kind of poised to see the legislation enacted
7 into law and probably with an eye to creating a
8 good record for that and during the time when
9 there was no exemption, at least one of the
10 carriers significantly restricted its policy.

11 So we think there's no substitute for
12 having a guaranteed right.

13 MR. DAMLE: Which carrier was it that
14 restricted the --

15 MR. SLOVER: It was AT&T.

16 MR. DAMLE: Okay. All right. So moving
17 on to sort of the kind of dispute that remains
18 among at least the people that are arrayed here as
19 between -- as I understand it, there's just sort
20 of a dispute about the scope of any exemption we
21 should grant.

22 So one question I have for you is: one
23 thing I didn't see in your proposal was a
24 limitation to used cell phones and tablets, which
25 is something that we have in the existing

1 exemption. It says that it has to be a used
2 wireless telephone handset.

3 And so is that -- is that something --
4 is that purposeful? Are you meaning to allow
5 circumvention of new handsets now?

6 So I wonder if you could address that.

7 MR. SLOVER: Sure. And I was going to -
8 - I was just about to get to sort of --

9 MR. DAMLE: Okay.

10 MR. SLOVER: -- why our exemption is
11 different --

12 MR. DAMLE: Sorry. I'm jumping ahead.

13 MR. SLOVER: -- from the others.

14 No. That's okay.

15 And I -- maybe I can explain it more
16 fully once I get to that point.

17 But my answer to you is a couple of
18 things. One, imposing conditions or restrictions
19 on the right to unlock makes it difficult from an
20 ordinary consumer's perspective. Because what
21 that means is here's a proof requirement. You've
22 got to be confident that you can prove this in
23 order to be protected from potential civil and
24 criminal liability.

25 And I think it's going to be difficult

1 for a consumer to know whether a phone has been
2 used or how it's been used in the past. All
3 they're going to know is that they've got a phone
4 that they've obtained, as far as they know, from a
5 lawful avenue and they want to unlock it and use
6 it on a new network.

7 So that's one thing.

8 The other thing is that there's one
9 situation where at least one of the definitions of
10 "used" is that it's been previously activated on a
11 wireless network. And so even if you could
12 satisfy the proof requirements, there's one
13 situation where we think consumers should have the
14 latitude to part with a phone before that happens.
15 And that's a situation where, under the contract
16 that I've got now, you -- you get a phone for a
17 certain period of time and then you're allowed,
18 when you renew your contract, to get a new phone.
19 And that's one of the incentives for renewing.

20 Well, maybe you're a guy like me who's
21 60 years old, and most of what you do is use your
22 phone to make calls and send e-mails, and your
23 teenager or your teenage nephew really likes the
24 full array of what the newest phone can do.

25 So rather than upgrade yourself to that

1 new phone, you're just going to keep using the one
2 that you've been using. But you essentially get
3 the new phone for free as part of the package. So
4 it doesn't make sense to give it up. So you take
5 it and you pass it on to your nephew.

6 MS. CHARLESWORTH: Is that -- I'm sorry.
7 But my experience, you know, is that usually
8 you're under contract, you go in with your old
9 phone under the contract, you have to hand that
10 one in and you get a new one that's another
11 subsidized phone under the contract.

12 I mean, I'm not familiar -- are you
13 saying there are actual -- and there may be. So
14 it's -- you know, but what kind of -- when would
15 you encounter a situation where you were -- had
16 both phones and the second one wasn't being
17 subsidized?

18 MR. SLOVER: You mean the new phone
19 wasn't --

20 MS. CHARLESWORTH: Well, I'm saying, if
21 I have -- if I -- I mean, correct me where I'm
22 wrong in this scenario.

23 I have, say, an iPhone 5. I want an
24 iPhone 6. I believe, if I went to my carrier and
25 took my iPhone 5 in and said I want a 6, they'd

1 say, "Yeah, you can have this. You've finished
2 your contract for the 5, but give us the 5 back"
3 or at least the 6 would then be subsidized and
4 under contract.

5 I'm just -- I'm just curious to know
6 from anyone on the panel whether there are -- and,
7 you know -- whether there are scenarios where you
8 would end up with a new, unsubsidized phone that
9 hadn't been activated with the carrier.

10 MR. SLOVER: Well, it might --

11 MS. CHARLESWORTH: The scenario you're
12 talking about, which is not familiar to me.

13 MR. SLOVER: It might very well be
14 subsidized. And the times that we've done this
15 before as a family, they have been subsidized.

16 It's a hidden subsidy that's part of the
17 -- of the monthly payment that we make.

18 MS. CHARLESWORTH: Right.

19 MR. SLOVER: And there are new models
20 now -- new kinds of service contracts that have
21 evolved in the last year or two or three that have
22 a different arrangement where the subsidy is more
23 transparent. But they still have the ones where
24 it's not transparent.

25 And in those situations, if you -- I

1 mean, you could say, "Well, thanks. But I don't
2 need a phone." But that wouldn't change your
3 monthly payment.

4 I mean, it would under some of the new
5 ones. But in some of the old ones, it doesn't
6 change it.

7 So what we think consumers should be
8 able to do is to say, "Okay. I'm going to take
9 that phone that you're requiring me to pay for.
10 I'm going to take it. But I don't want to use
11 it."

12 MS. CHARLESWORTH: Is it under contract?

13 MR. SLOVER: "I'll let somebody else use
14 it."

15 MS. CHARLESWORTH: Is the new phone
16 under contract in your scenario?

17 MR. SLOVER: It's a service agreement.

18 MS. CHARLESWORTH: Right. So it's a --
19 presumably, it's a subsidized phone. So you're
20 saying -- I mean, then do you go and pay off the
21 contract? How does that work? What's your
22 obligation to the carrier vis-a-vis the new phone?

23 MR. SLOVER: Well, your obligation is
24 under the contract. You've --

25 MS. CHARLESWORTH: So you can --

1 MR. SLOVER: -- agreed to have service
2 with that carrier for a two-year period or however
3 long it is.

4 MS. CHARLESWORTH: Right.

5 MR. SLOVER: And if you don't continue
6 the service for that period of time, there's an
7 early termination fee.

8 There are contractual obligations that
9 don't have to do with the lock on the phone.

10 MS. CHARLESWORTH: But would they let
11 you walk out of the store with a phone that they
12 didn't activate to their network? I mean, if I
13 were -- and this is -- I mean, if you're AT&T and
14 you're handing out a subsidized phone, why would -
15 - why would your policy permit you to hand it out
16 without activating it, which is -- we're going
17 back to the definition of "used" here, which you
18 objected to.

19 But, I mean, it seems it me that the
20 policy -- most policies -- and, again, people can
21 feel free to dispute this -- that if it's a
22 subsidized phone, they're probably not handing you
23 a phone that they're not activating and letting
24 you walk out of the store, even if you're under
25 contract.

1 MR. SLOVER: Well, if that's the kind of
2 deal that they want to offer, then that's the deal
3 that they should offer. And other carriers may
4 offer a different deal.

5 MS. CHARLESWORTH: But do they? That's
6 what -- we're trying to find out what they
7 actually do because you're objecting to the
8 definition of "used," and the bigger issue here is
9 the -- you know, we have comments from TracFone.
10 They're not here today. But the bulk situation
11 where people are buying up phones, subsidized
12 phones -- and I want to hear more about this too -
13 - and then reselling them in a way that's -- at
14 least TracFone thinks is inequitable.

15 But you're positing a scenario where you
16 could -- you're disputing a definition based on a
17 scenario that I'm not sure exists in the real
18 world. And so that's what I'm trying to
19 understand, that you could walk out of -- as an
20 individual consumer, you could walk out of AT&T
21 with a contract phone that hadn't been activated.

22 MR. SLOVER: Well, what we're -- what
23 we're hoping will be the result is that there will
24 be flexibility in the kinds of contracts that can
25 be made available to consumers and the kinds of

1 ways that they can get phones and that there's not
2 a barrier that doesn't need to be there that says,
3 you know --

4 MS. CHARLESWORTH: Well, there --

5 MR. SLOVER: -- we're prohibited under
6 the DMCA, as its been interpreted, from allowing
7 you to walk out of here with a phone that hasn't
8 been activated.

9 MS. CHARLESWORTH: They would just let
10 you buy an unlocked phone, right? You would pay
11 the \$700.

12 I mean, that would be the answer --
13 there is a -- I mean, a lot of -- some carriers do
14 let you do that.

15 In other words, if they're going to let
16 you walk out of the store with a phone that's, you
17 know -- I mean, they can sell you an unlocked
18 phone, and then there's not a concern about
19 fulfilling your contract and all that.

20 So that -- you know, they can do that
21 regardless of Section 1201 today.

22 MR. SLOVER: Right. Those that want to
23 can offer that.

24 But if they're going to lower the price
25 of the monthly service contract in connection with

1 that, then that would be something that a consumer
2 could weigh the pros and cons of which way to go.

3 But if the consumer sees an advantage to
4 being on an extended contract, they know they're
5 going stay with the same carrier because they've
6 been with that carrier for years and they like
7 that carrier, they should be able to keep their
8 old phone. And the deal that they've signed up
9 for should not require them to pay for a phone
10 that they don't want just because they are
11 constrained from passing that phone along to
12 somebody else.

13 MS. CHARLESWORTH: Okay.

14 MR. DAMLE: So just to be clear, I mean,
15 you object to the current exemption, as it was
16 reinstated by -- I mean, you don't think the
17 current exemption, as was reinstated by Congress,
18 is sufficient?

19 MR. SLOVER: We think, as a practical
20 matter, most of the phones that are going to be
21 involved here are going to be used phones. But we
22 -- in advocating before Congress and in advocating
23 in past triennial reviews, we have urged that the
24 exemption not be limited to used phones.

25 So our position is the same as it's

1 been.

2 MR. DAMLE: Okay.

3 MS. CHARLESWORTH: And how do you
4 respond to the TracFone concern?

5 MR. SLOVER: Well, we are not in favor
6 of illegal bulk trafficking, and we're not talking
7 about illegal bulk trafficking here. We're
8 talking about something that an individual
9 consumer would do with the phones that they obtain
10 for themselves or for their immediate family
11 members on a contract that they've entered into
12 with a carrier.

13 MS. CHARLESWORTH: Can I just go back to
14 your scenario? Because under your -- let's say
15 you purchase a phone from -- you get your new
16 phone from AT&T and you in your head think, "I --
17 you know, I'll pay off my contract, but I'm going
18 to -- I want to unlock this and switch it right
19 away. I'm going to go from AT&T to the next
20 store."

21 You could have AT&T activate it and then
22 not -- I mean, in other words, you could easily
23 fall under the "used" definition if you simply
24 have it activated by AT&T before you walk next
25 door and have a new carrier unlock it and activate

1 on their network.

2 So that's why I'm not -- I mean, it's
3 just not that hard -- I mean, that's -- since
4 you're getting the phone right there anyway,
5 there's really no particular burden in doing that
6 if you want to meet the "used" definition.

7 But the reason that people have proposed
8 that definition, as I understand it, is to help
9 prevent or at least exclude the kind of bulk
10 trafficking scenario, which is a concern in the
11 record.

12 So there's sort of that -- as I -- and
13 they can speak to that more directly than I can.
14 But that's the -- that's what they're responding
15 to. So, like, I just don't really see the -- I
16 don't -- I don't see why this is so limiting to,
17 you know -- to consumers who want to switch even
18 if they're, frankly, going to break their
19 contract.

20 MR. SLOVER: Well, I think working
21 through the hypotheticals that you've laid out...

22 I've got an iPhone 5. I have the
23 opportunity to get an iPhone 6 or I have an
24 opportunity for virtually nothing to get an iPhone
25 5S when I go back in. And I decide that the

1 iPhone 5S is not that much better than the iPhone
2 5, so I'm going to keep the one that I've got.

3 But I'm basically being offered a free
4 iPhone 5S. So I would like to give that to my
5 nephew who lives in a different city. And he's
6 going to hook it up with somebody different. It's
7 going to be on a different account than mine.

8 So what the hypothetical that you're
9 describing would be is that I would get the phone
10 from AT&T, I would hook it up, I would transfer
11 all of my data and my phone number and everything
12 to my new iPhone 5S, and then I would go back in
13 the next day and say, "I want you to transfer
14 everything back into my old phone."

15 So theoretically that could happen. It
16 wouldn't be all that hard.

17 MS. CHARLESWORTH: And your new --

18 MR. SLOVER: But why should the consumer
19 have to do that if the end result is the same?

20 MS. CHARLESWORTH: So how would you
21 propose to address the bulk issue differently?

22 I mean, in other words, assuming that's
23 a legitimate concern that people are misusing --
24 might misuse the exemption or whatever TracFone --
25 you know it's their concern. But it has been a

1 perennial concern, this -- I mean, how would you
2 address it?

3 MR. SLOVER: So Consumers Union
4 definitely agrees that it's a legitimate concern.

5 I think the question here is: is it a
6 copyright concern?

7 So from the bulk unlocking perspective
8 and what the problems are there, TracFone has a
9 number of alternative legal remedies at its
10 disposal that its used.

11 And from our perspective, the question
12 really is: Should the average consumer continue
13 to have DMCA liability?

14 MS. CHARLESWORTH: Well, I mean, is it a
15 copyright concern that the person has to go to
16 AT&T and switch the data back?

17 I mean, a lot of this stuff is not
18 really -- you know, a lot of the things we talk
19 about or the value of recycled phones and whether
20 their price is different because you can unlock
21 them -- you can say they're not copyright
22 concerns, but they're all part of this -- this
23 particular exemption that we're talking -- I mean,
24 they're concerns that are raised.

25 I understand there may be other legal

1 avenues. But, like, let's assume that they think
2 that 1201 is an important factor in this, which
3 they clearly do.

4 I mean, is there a way you could write
5 the exemption to exclude that behavior that you
6 would be willing to agree to? Because the other
7 parties have come to, I think, some version of an
8 understanding on this.

9 MR. SLOVER: Well, I don't want to speak
10 for the other parties as well --

11 MS. CHARLESWORTH: No.

12 MR. SLOVER: -- because I -- what I've
13 noticed, I think there is still a difference
14 between what CCA and TracFone have proposed versus
15 what ISRI has proposed with the "used" exemption
16 with the addition of the term "used" as well.

17 So I think that there's some issues
18 there.

19 MS. CHARLESWORTH: Okay. Well, why
20 don't we move on and hear from the other parties.

21 Mr. Lazarus?

22 MR. LAZARUS: Okay. So we represent
23 Competitive Carriers Association. We will
24 significantly scale back our open and just sort of
25 try and get to a couple of paragraphs.

1 We -- Competitive Carriers Association
2 is the nation's leading association for
3 competitive wireless providers and stakeholders
4 across the country. CCA's membership includes
5 more than a hundred wireless providers ranging from
6 small rural providers serving fewer than 5,000
7 subscribers to regional and national providers
8 serving millions of customers.

9 As a result, CCA has a keen interest in
10 ensuring that all wireless subscribers have access
11 to cutting-edge handsets and wireless devices
12 available today for use on networks of their
13 choice.

14 CCA believes that the use of wireless
15 devices to connect to different wireless networks
16 represents a noninfringing use and not granting an
17 exemption will likely result in adverse harm to
18 consumers both in the present day as well as
19 within the next three years.

20 Accordingly, CCA strongly supports an
21 exemption allowing consumers to unlock all of
22 their devices that connect to wireless
23 telecommunications networks in order -- in order
24 to associate such devices with the network of
25 their choosing, which CCA originally proposed via

1 four different petitions before this office and
2 comments in the record.

3 This protection should apply not only to
4 handsets and tablets but to all wireless devices
5 that have the potential to connect to a
6 telecommunications or information services
7 network.

8 Because this proceeding is forward-
9 looking, an exemption should allow consumers the
10 ability to unlock any relevant device and not be
11 subservient to the will of one carrier or
12 manufacturer.

13 In addition, as directed by Congress,
14 the exemption should not limit who may provide
15 assistance to unlock a device and, therefore,
16 should allow an agent of the consumer, whether it
17 be a person or a different wireless provider, to
18 perform the unlocking procedure, just as a
19 locksmith may unlock an individual's car or home
20 when they do not have the necessary key.

21 Now, while there has been near universal
22 support for an exemption of this nature, one party
23 did express limited support, seeking additional
24 protections related to subsidies, TracFone.

25 Although CCA believes that its original

1 proposed exemption is consistent with the
2 Copyright Office's mandates concerning
3 circumvention, in light of the Register of
4 Copyright's recent testimony before the Committee
5 on the Judiciary where she expressed a desire for
6 Section 1201 to be amended to provide that
7 existing exemptions will be presumptively renewed
8 during the ensuing triennial period in cases in
9 which there is no opposition, CCA worked
10 diligently with the sole opponent, TracFone, to
11 its proposed exemption to reach a compromise on a
12 modified proposed exemption.

13 These modifications will continue to
14 properly enable users to take control over the use
15 of their wireless devices and permit them the
16 choice of which network they will be connected to
17 while also helping to ensure that such an
18 exemption may not be easily exploited by
19 traffickers and to steal subsidies pursuant to
20 contracts.

21 MS. CHARLESWORTH: Okay. And can you
22 explain, just to home in on the issue -- be
23 specific for the record about how you -- the part
24 of your proposal that protects against bulk
25 unlocking and why -- and how it does that?

1 MR. LAZARUS: Sure. So what we tried to
2 do is come up with a formulation similar to what I
3 would call the contract law formulation.

4 A number of our member carriers have
5 subsidies. You can buy a phone from them for a
6 two-year contract. You can buy a phone from them
7 via a device installment plan. So we're not blind
8 to that concern.

9 And what we tried to build into this
10 exemption was the idea that, for the original
11 owner, that you would not be able to go unlock
12 your phone unless you adhered to the -- to the
13 terms of the contract that you had. So
14 essentially, you walk into AT&T, you buy a phone
15 for two years -- under a two-year contract. In
16 month three, you shouldn't necessarily be able to
17 just go get your phone unlocked.

18 So that's how we tried to bridge the gap
19 with TracFone.

20 Now, what we also don't believe -- so
21 when you go into -- as far as liability is
22 concerned, we do believe that we should follow
23 what Congress asked this office to do, which is
24 essentially, if you take that phone and bring it
25 into a particular carrier, that carrier should be

1 able to unlock it. We don't think there should be
2 any liability surrounding that.

3 Any liability should hold to the -- what
4 I would call the original owner and their original
5 obligations to their original carrier.

6 MR. DAMLE: So I just want to sort of
7 test a few points here.

8 MR. LAZARUS: Mm-hmm.

9 MR. DAMLE: One is -- well, you
10 mentioned that it's a two-year contract. There
11 are often termination fees that you can pay to get
12 out from your contract.

13 MR. LAZARUS: Sure.

14 MR. DAMLE: I take it that, if someone
15 pays the termination fee -- they're leaving the
16 state, they're leaving the country, they don't
17 want to -- they just want to terminate their
18 contract and take their phone.

19 MR. LAZARUS: Yep. Absolutely. I think
20 that's built into our proposed exemption already.
21 It's really -- once you pay off the ETF, the early
22 termination fee, your obligations to the original
23 carrier terminate.

24 So at that point, you should be able to
25 take your phone and unlock it wherever you want.

1 MR. DAMLE: Okay. So one of the
2 concerns that ISRI has raised -- I don't want to
3 put words in their mouth -- but as I understand
4 it, that it's unclear who the owner is.

5 So if I own a phone and then -- if I buy
6 a phone sort of on eBay and it's locked, I don't
7 necessarily know where -- whether the original
8 owner has satisfied all of their obligations to
9 the -- to that carrier that the phone is locked
10 to.

11 So do you have -- do you have a response
12 to that concern? Is there --

13 MR. LAZARUS: Well, we --

14 MR. DAMLE: Is there a solution to that
15 concern?

16 MR. LAZARUS: We were concerned with the
17 original owner.

18 MR. DAMLE: Right.

19 MR. LAZARUS: So as far as we're
20 concerned, if it goes to a second -- a second
21 owner at that point, we don't think that owner
22 should have to track down, you know, what has been
23 going on, you know, two owners before, three
24 owners before. Right?

25 So it's essentially a good-faith

1 obligation attached to the original owner.

2 MR. DAMLE: Right.

3 MR. LAZARUS: So we're not in -- I don't
4 view us as in disagreement. I think we all view
5 this the same way.

6 That second owner should just be able to
7 go get their phone unlocked without having to
8 worry about, "Okay. There were three owners
9 before. Do we have to try and figure out what
10 happened there?"

11 MR. DAMLE: Okay. So -- okay. So a
12 slightly -- so let's say I want to give it to a
13 family member. I want to give my phone to the
14 family -- to a family member.

15 MR. LAZARUS: Mm-hmm.

16 MR. DAMLE: Say it's not a member of my
17 immediate family; it's my nephew. What about in
18 that scenario? I mean, is the subsequent owner in
19 that scenario required to satisfy the contract?

20 I mean, I'm giving you hypotheticals to
21 test the limits of --

22 MR. LAZARUS: Sure. I think in that
23 particular situation -- we don't have a particular
24 view on it. I think -- again, once -- we're
25 trying to avoid a situation where you do have to

1 worry about an obviously much closer call -- you
2 know, if the dad buys the phone and gives it to --
3 you know, a husband buys the phone and gives it to
4 the wife, for instance. Can she get around her
5 contract?

6 We would view that as no. Most of our
7 member carriers would view that particular
8 situation as no.

9 But, again, I think we view that more as
10 a contract claim, more as a contract matter rather
11 than necessarily a DMCA matter.

12 MR. DAMLE: So if we were to make clear
13 -- just going back to sort of the -- like, you
14 know, the arm's length kind of scenario.

15 MR. LAZARUS: Mm-hmm.

16 MR. DAMLE: If we were to make clear
17 that subsequent owners would not be required to
18 assess whether the original owner has satisfied or
19 -- his or her contract obligations or whether
20 those contract obligations are waived, you would
21 be fine --

22 MR. LAZARUS: Absolutely. Yes.

23 MR. DAMLE: Okay. That's helpful.
24 Thanks.

25 MS. CHARLESWORTH: Did you have anything

1 else, Mr. Lazarus?

2 MR. LAZARUS: No.

3 MS. CHARLESWORTH: You're good for now?

4 MR. LAZARUS: I am.

5 MS. CHARLESWORTH: Mr. Harris?

6 MR. HARRIS: Thank you very much. I'm
7 appearing today in support of ISRI's proposed
8 exemption for class 11, unlocking the wireless
9 telephone headsets.

10 I want to make two introductory remarks
11 and then turn the presentation over to our two law
12 student counsel.

13 ISRI is a trade association representing
14 more than 1600 processors, brokers, and industrial
15 consumers of scrap commodities. However, among
16 our members are recyclers of used phones and
17 tablets. These are the companies that lawfully
18 acquire used, unwanted phones from individual and
19 corporate owners, refurbish these phones, and
20 resell them back into the marketplace.

21 The work of recyclers provides important
22 public and economic benefits by enhancing the
23 value that consumers can receive when they sell
24 the used phones, increasing the number and variety
25 of used phones available for other consumers to

1 purchase and ensuring greater competition in the
2 wireless device and carrier marketplaces.

3 In order to achieve these benefits,
4 recyclers like our members need to be able to
5 unlock in bulk the phones they legally obtain. We
6 need a clear exemption to Section 1201 that
7 removes concerns about potential DMCA liability,
8 the risk of which is substantial in the current
9 law.

10 Only one party, as we've discussed,
11 TracFone, has objected to our and the other
12 proponents' proposed unlocking exemptions out of
13 concerns that the exemptions will permit illegal
14 phone trafficking.

15 Let me be clear. ISRI's members do not
16 engage in phone trafficking, and we do not in any
17 way condone such trafficking.

18 MS. CHARLESWORTH: Can I ask you a
19 question? I mean, I've always had -- this is --
20 there seems to be a couple different versions of -
21 - I don't know if they're all trafficking, in your
22 view.

23 MR. HARRIS: Right.

24 MS. CHARLESWORTH: But what TracFone was
25 describing was people, as I understood it, going

1 to a -- buy subsidized -- or phones that are
2 intended for -- to be locked to a carrier off of a
3 shelf at a discounted price, essentially
4 subsidized.

5 MR. HARRIS: Right.

6 MS. CHARLESWORTH: And then instead of,
7 you know, accessing that carrier or -- you know,
8 they sell them somewhere else with the -- you
9 know, and sort of an arbitrage on the phones.

10 Is that a -- is that a scenario that
11 you're familiar with? And can you comment on
12 that?

13 And then there was a sort of second
14 scenario. I'll just -- it will be a two-part
15 question where there seemed to be sort of truly a
16 black market in phones that were meant to, say, go
17 to carriers for subsidized plans but somehow fell
18 into the wrong hands.

19 And I'm just curious to know more about
20 -- about the sort of that -- those
21 issues:

22 trafficking and the stuff that TracFone
23 was talking about.

24 MR. HARRIS: Sure. As to the first
25 question, I mean, we'll take their word for it.

1 That's not our concern. That's not our issue.

2 And we concede the notion that applying
3 the exemption for used devices really addresses
4 almost all of our concerns.

5 Our members don't deal in recycling new
6 phones or phones that you buy at a store. That's
7 just not the business model. That's not what they
8 do. That's not what we're here to advocate on
9 behalf of.

10 As far as the black market or illicit
11 trade of phones in the alternative, also that's
12 not the behavior that we're advocating for. We're
13 looking at legitimate contractual relationships
14 where a recycler will go and purchase that phone
15 or that tablet from either a consumer or a
16 business entity. And then they own those phones
17 and they want to refurbish them and do what they
18 need to do to resell them back in the market.

19 And that's all under a very transparent,
20 you know, very legally valid contractual type of
21 arrangement.

22 MS. CHARLESWORTH: Do you think there
23 needs to be a definition of "used" in the
24 exemption? Or is "used" sufficient, from your
25 point of view, to explain what's exempted?

1 MR. HARRIS: Well, I think certainly a
2 definition could be helpful depending on what it
3 is. Certainly, we're comfortable with what appears
4 to be where that definition is going.

5 MS. CHARLESWORTH: Meaning saying it had
6 been -- what is it? -- "lawfully acquired and
7 activated on the wireless telecommunications
8 network of a carrier"?

9 MR. HARRIS: Yeah. That language would
10 be fine for us.

11 MS. CHARLESWORTH: That would work for
12 you?

13 MR. HARRIS: That would work.

14 MS. CHARLESWORTH: Okay.

15 MR. DAMLE: Sorry. And the language --
16 so I think that may have been language that you
17 had put forward at one point.

18 But the language proposed by CCA and
19 TracFone in their reply comments, do you have any
20 thoughts about that language?

21 MR. HARRIS: As far as the "original
22 owner" concept or --

23 MS. CHARLESWORTH: Well, it's more tied
24 to fulfilling --

25 MR. DAMLE: Fulfilling the contract.

1 MS. CHARLESWORTH: -- the contract.

2 MR. DAMLE: Not being used for unlawful
3 purpose, theft and fraud -- the device was not
4 obtained by theft or fraud.

5 MR. HARRIS: Yeah. I mean, and -- my
6 colleagues here will get -- will get into this as
7 well.

8 MR. DAMLE: Okay. Fair enough.

9 MR. HARRIS: So maybe I'll punt to them.
10 But I do think that overall there is a path that
11 we can move forward here that would certainly
12 address our issues.

13 MS. CHARLESWORTH: Okay. Thank you, Mr.
14 Harris.

15 Mr. Weissenberg?

16 Ms. Long?

17 MS. LONG: Hi. So we understand that
18 TracFone's initial proposal as well as
19 TracFone and CCA's compromise both contain a
20 requirement saying that you have to -- the
21 original owner has fulfilled the contract
22 obligations or recouped -- allowed the carrier to
23 recoup any subsidy it may have provided in the
24 handset price.

25 But for ISRI's members, that language

1 would be impractical. It would make it impossible
2 for them to unlock the phones they receive because
3 ISRI is not the original owner. They're a
4 subsequent owner, and they acquire the phone
5 lawfully, but they have no way of figuring out
6 whether the original owner has satisfied its
7 contract obligations.

8 MR. DAMLE: So the colloquy that I had
9 with Mr. Lazarus where I suggested we might be
10 able to kind of clarify that subsequent owners
11 would not have that obligation, would that satisfy
12 your concern?

13 MS. LONG: Yes.

14 MS. CHARLESWORTH: Okay. You can
15 continue.

16 Ms. Long, did you have anything further
17 to add or --

18 MS. LONG: That's all I have.

19 MS. CHARLESWORTH: Okay. And, Mr.
20 Weissenberg, did you want to say anything for the
21 record?

22 MR. WEISSENBERG: Good afternoon and
23 thank you again for allowing us to testify before
24 you today.

25 Again, my name is Brian Weissenberg, and

1 I'm a Stanford law student at the Stanford IP and
2 Innovation Clinic, representing Petitioner ISRI.

3 In my short time, I want to make two
4 brief but important points about the Unlocking Act
5 which was enacted in 2014 and which helps guide
6 the unlocking portion of this rulemaking.

7 First, as Mr. Slover already discussed a
8 bit, the Unlocking Act demonstrates that Congress
9 and the President believe that any copyright
10 concerns should yield to the pro-consumer benefits
11 of unlocking one's phone and moving it onto a
12 different carrier.

13 While ISRI submitted a full and careful
14 Section 117 analysis and fair-use analysis in our
15 initial comment, we believe that analysis is
16 ultimately unnecessary because the Unlocking Act
17 expressly allows unlocking by owners of mobile
18 devices regardless of whether they own the
19 underlying copies of software on those phones.

20 The act specified and the Copyright
21 Office itself affirmed in its notice of inquiry
22 that future unlocking exemptions will apply to
23 phone owners, not owners of the copies of the
24 software.

25 But second and most importantly, we

1 believe the Unlocking Act itself also allows bulk
2 unlocking.

3 As just discussed, the Unlocking Act
4 specifically allows device owners to unlock their
5 phones. Recyclers are the lawful owners of those
6 mobile devices they receive and seek to unlock.

7 This is also confirmed in the
8 legislative history of the Unlocking Act.

9 Now, you may recall that at one point
10 there was a clause in the bill that mentioned bulk
11 unlocking in a way that many were concerned might
12 be interpreted to deny unlocking benefits to bulk
13 unlockers.

14 But after much debate, that language was
15 ultimately removed and does not appear in the
16 Unlocking Act that was signed into law by
17 President Obama.

18 But what's more telling is that, even
19 when that language was in the bill, Representative
20 Goodlatte, the bill's primary sponsor, expressly
21 stated that the clause, quote, "is not intended to
22 impair unlocking by legitimate recyclers or
23 resellers," unquote.

24 But instead that language was targeted
25 at phone traffickers. So Congress made clear that

1 this act was intended to protect phone recyclers
2 like ISRI's members. In other words, we resell
3 used phones just like a used bookstore sells used
4 books, which the Librarian of Congress in 2010
5 stated would be a protected commercial activity.

6 Now, although we believe bulk unlocking
7 is covered by the Unlocking Act, we also believe
8 it is vital that such unlocking be explicitly
9 permitted in any new exemption to avoid any
10 ambiguity and uncertainty for recyclers.

11 Finally, I want to note Mr. Harris's
12 reminders that only one party, TracFone, opposes
13 the unlocking exemptions and add the important
14 fact that even TracFone says in its filing that it
15 supports an unlocking exemption so long as that
16 exemption expressly excludes any provision that
17 could be exploited by illegal traffickers to steal
18 subsidies and harm consumers.

19 So, really, the only real disagreement
20 at this stage of the rulemaking should be over the
21 precise scope and wording of an unlocking
22 exemption.

23 Now my colleague, Donna Long, will
24 answer that question describing how our proposed
25 exemption is carefully drafted so it will not

1 exempt illegal phone trafficking.

2 Thank you.

3 MS. CHARLESWORTH: Ms. Long?

4 MS. LONG: Hi. I'm Donna Long. I'm
5 with the Stanford IP and Innovation Clinic. We're
6 representing ISRI.

7 So I have two quick points about our
8 trafficking discussion so far.

9 First of all, TracFone has available and
10 regularly uses a variety of noncopyright legal
11 claims to stop traffickers and seeks recovery for
12 any harm that it would suffer from trafficking.

13 So the DMCA is not only inappropriate
14 but unnecessary for the trafficking concern.

15 MS. CHARLESWORTH: But can I just -- I
16 mean, isn't it true that they also have
17 successfully used the DMCA, 1201, to address
18 trafficking issues?

19 MS. LONG: Yes. They have successfully
20 filed lawsuits with the DMCA as well as up to 10
21 or 12 other claims that they've won on all of
22 them.

23 MS. CHARLESWORTH: Right. But they --
24 okay. Continue.

25 MS. LONG: And second, I wanted to

1 emphasize that ISRI's proposed language was
2 carefully crafted so that it could not be
3 construed to permit phone trafficking. Our
4 language would only allow unlocking of used phones
5 and, as we said, that means phones that have been
6 lawfully acquired and activated on the wireless
7 telecommunications network of a carrier.

8 So TracFone's new phones that are being
9 unlocked in the process of this legal trafficking
10 would never fall within the scope of that
11 language.

12 As TracFone has described in its
13 trafficking litigation, the scenario that they are
14 trying to address is where trafficked phones are
15 bought at a retail outlet then resold new without
16 ever being activated on a network. And,
17 therefore, trafficked phones would never fit the
18 definition that ISRI has proposed about "used."

19 MS. CHARLESWORTH: Okay. Did you have a
20 question, Mr. --

21 MR. DAMLE: I hit the bell. Sorry about
22 that.

23 So I actually wanted to go back to Mr.
24 Lazarus, if that's okay.

25 MS. CHARLESWORTH: No. No. Go ahead,

1 Mr. Damle.

2 MR. DAMLE: So one question I had --
3 just looking through the elements of your proposed
4 language, one question I had is why it's necessary
5 to include -- to specifically exclude devices
6 obtained by theft or fraud. I mean, that's
7 something that we don't have in our current
8 exemption, and maybe this is not a position that
9 you've been taking and this may have been from
10 TracFone.

11 But I'm sort of curious if you can just
12 sort of explain the reasoning behind putting that
13 explicitly in the exemption.

14 MR. LAZARUS: Sure. And as you note,
15 this was part of a -- sort of a negotiated way --

16 MR. DAMLE: That's what I --

17 MR. LAZARUS: -- to get TracFone to --

18 MR. DAMLE: Yes.

19 MR. LAZARUS: -- to not be opposed in
20 this proceeding.

21 I mean, I think most wireless carriers,
22 for the most part, are actually able to tell
23 whether or not a phone has been stolen before they
24 reactivate it on their network. I know some of
25 the carriers are able to do that.

1 So, again, it was part of the negotiated
2 settlement, and we didn't view it as -- again, if
3 you're looking at some of TracFone's concerns, you
4 know, theft is one of their main concerns. So...

5 MR. DAMLE: Okay. And go back to the
6 sort of subsequent owner point. You can imagine a
7 scenario -- again, going back to eBay -- where an
8 innocent purchaser buys a -- buys a cell phone
9 from eBay or one of ISRI's members -- you know,
10 Gazelle or something.

11 MR. LAZARUS: Sure.

12 MR. DAMLE: Gets a cell phone and
13 doesn't know whether it's been stolen or not.

14 MR. LAZARUS: Mm-hmm.

15 MR. DAMLE: So do you have the same
16 position with respect to that situation?

17 MR. LAZARUS: CCA does, yes.

18 MR. DAMLE: And do you know if TracFone
19 --

20 MR. LAZARUS: I don't think I'm in a
21 position to speak for TracFone.

22 MR. DAMLE: Okay. All right. And then,
23 again, the same thing with respect to the
24 specification that it's for -- that it not be for
25 "any unlawful purpose."

1 Can you give me a sense of sort of what
2 the unlawful purposes are? Is it, again, just
3 criminal trafficking of --

4 MR. LAZARUS: That's exactly right.

5 MR. DAMLE: Okay.

6 MR. LAZARUS: Again, trying to fit a
7 negotiated settlement that -- or a negotiated
8 proposal that would fit what CCA was looking for
9 and try to resolve some of TracFone's concerns in
10 this proceeding. And the idea that it would be
11 for unlawful purpose, I think, might have come
12 from their original proposal as well.

13 MR. DAMLE: Okay. And is it your view
14 that the proposal, as you've drafted it, is meant
15 to cover bulk unlocking of used cell phones? Is
16 that something that you've -- of used cell phones,
17 not new ones.

18 MR. LAZARUS: I think, if you look at it
19 as drafted, I don't think the language difference,
20 if you look at -- you know, what we were concerned
21 about was -- again, sort of the contract principle
22 of, okay, you buy a cell phone from one of our
23 members, you know, them trying to break their
24 contract. That's not what seems to be going on
25 with the formulation that ISRI is looking for.

1 MR. DAMLE: Right.

2 MR. LAZARUS: So I don't think there's
3 that much disagreement between the two. And I
4 don't think we were trying to get at stopping what
5 I would call legalized bulk unlocking.

6 MR. DAMLE: Right. Okay. All right.
7 That's helpful.

8 MS. CHARLESWORTH: Mr. Slover?

9 MR. SLOVER: Yes. I just wanted to
10 clarify that the point that Mr. Lazarus has
11 brought up and that your colloquy engaged in, the
12 difference between the original owner of the phone
13 who got it in connection with the contract with
14 the carrier and subsequent owners who don't have a
15 clear knowledge -- a firsthand knowledge of how
16 the phone was originally acquired, I think, is
17 very important.

18 That was not clear to us as we read any
19 of the proposals. If that's clarified, that takes
20 care of, from our perspective, a big part of our
21 concern, which was how are you -- how is the
22 consumer who acquires this from eBay or even a
23 bulk unlocker going to know the provenance of the
24 phone, tracing it all the way back to its origin.

25 So I think that would be very helpful.

1 We detailed in the statement that I was
2 going to give and that I didn't finish some of the
3 things that we saw as preferential in our proposal
4 to the others. And one of them was about the
5 problems of proof that would be required of a
6 consumer, particularly one of the subsequent
7 consumers.

8 With your permission, I'd like to offer
9 it in writing after the proceeding just so that
10 you can see what I would have said. And then, if
11 we have a chance to follow up on that, if you're
12 taking additional written statements, we'd expand
13 on that.

14 MS. CHARLESWORTH: Well, I think -- we
15 hadn't planned on another full round of comments.

16 Are you saying -- what is it -- is there
17 something you want to share with us here in terms
18 of what you would have said?

19 MR. SLOVER: Well, in a nutshell --

20 MS. CHARLESWORTH: Because, to be
21 honest, I mean, you know, when -- you know, we'd
22 have to reopen -- you know, and in limited cases,
23 we may ask targeted questions. So I won't rule
24 out the possibility we would ask a limited
25 question afterwards that would address some of

1 these issues.

2 But I think if you have something to say
3 on that issue, I would recommend that you say it
4 now.

5 MR. SLOVER: Okay. Well, this is -- I
6 will.

7 This is the first that we are hearing
8 about the possibility of distinguishing between
9 the consumers and how they would be affected.

10 We'd hope to have a chance to consider
11 that more fully. It sounds like a promising idea,
12 but it's hard to do that on the fly.

13 But the main thing that I wanted to --
14 that was in my earlier statement that I'd like to
15 say is that the proof requirements of, you know,
16 whether a phone is going to be used for an
17 unlawful purpose -- you know, how is an ordinary
18 consumer going to know what's lawful and what's
19 unlawful?

20 You know, it's -- the way that it's
21 written, it says "including abusing a subsidy,"
22 but it's -- you know, including but not limited
23 to.

24 So it could be anything. And so that's
25 why we think the cleaner proposal, like we've done

1 or like ISRI has done, is superior to one that
2 loads up too many conditions which really turn
3 into proof requirements for an ordinary consumer
4 to be comfortable that they're complying with the
5 law.

6 MS. CHARLESWORTH: Okay. Mr.
7 Weissenberg?

8 MR. WEISSENBERG: Just one quick
9 comment. ISRI agrees with Mr. Lazarus and Mr.
10 Slover that the responsibility for those subsidies
11 should lie with the original owner.

12 But to the extent that the Copyright
13 Office adopts another definition that we propose,
14 we just ask that they make it very explicitly
15 clear that it applies to lawful bulk recyclers
16 like us, so -- to leave out any ambiguity.

17 Thank you.

18 MS. CHARLESWORTH: Okay. Do we have any
19 further questions?

20 Mr. Cheney?

21 MS. CHENEY: Yes. We haven't talked
22 about the sort of mail-order phones that are
23 available sort of through secondary -- not
24 directly from carriers, such as Overstock and
25 others that you can go onto their website and you

1 can purchase -- you can select it from different
2 carriers.

3 Is that covered as well under what you've
4 proposed in these possible exemptions where they
5 might get the phone and then you have to call
6 after you receive it to actually connect to the --
7 to activate and you're not activated -- the phone
8 is not activated when you receive it in the mail,
9 but it's activated once you call and activate it
10 after you've received it.

11 Is this covered in this situation?

12 MR. LAZARUS: Yes. I would think -- I
13 think it's covered by our formulation. I think
14 the idea -- just use Amazon as an example. You
15 can buy an unlocked phone through Amazon or you
16 can buy a locked phone through Amazon tied to a
17 particular wireless network.

18 MS. CHENEY: Right.

19 MR. LAZARUS: And so it's whatever
20 choice you would make. But I think that would be
21 covered by our formulation.

22 MS. CHENEY: Is it covered by Consumer
23 Union?

24 MR. SLOVER: It would be covered by ours
25 because ours extends the protection to the owner

1 of the device.

2 MS. CHARLESWORTH: Does that answer your
3 question, Ms. Cheney?

4 MS. CHENEY: Yeah.

5 MS. CHARLESWORTH: Mr. Damle?

6 MR. DAMLE: So I just wanted to clarify
7 something about the tablet unlocking proposals and
8 that -- that those -- I just want to be clear
9 whether or not your proposals would limit those to
10 also used tablets, not new tablets.

11 Is there an issue -- like, is that -- I
12 assume the answer is yes, but --

13 MS. CHARLESWORTH: So you'd treat them
14 in the parallel fashion?

15 MR. DAMLE: Right.

16 MR. DAMLE: Mr. -- we're getting nods.
17 So, Mr. Weissenberg, do you want to speak on
18 behalf of ISRI?

19 MR. WEISSENBERG: Yes. ISRI is -- we're
20 seeking an exemption for used devices. That's
21 correct.

22 MS. CHARLESWORTH: Okay.

23 MR. WEISSENBERG: Yes.

24 MR. DAMLE: And Mr. Lazarus?

25 MR. LAZARUS: Yes. We would be fine

1 with this applying to both.

2 MR. DAMLE: And Mr. Slover?

3 MR. SLOVER: We do want the same
4 exemption to apply to all devices that fit within
5 the same function. And we would hope that you
6 would consider the one situation that we described
7 where we think there should be the option for
8 either if the market already is there or the
9 market were to evolve so that the consumer has the
10 choice to pass along the new phone.

11 MS. CHARLESWORTH: Right. But -- I'm
12 sorry. But just again, I mean, I think -- I'm not
13 aware that any carriers would, under that
14 scenario, let you walk out of the showroom with a
15 subsidized phone that they hadn't activated. Are
16 you?

17 MR. SLOVER: Well, one of the -- no, I'm
18 not. But one of the problems with the exemption
19 in the past is that it has rigidified the business
20 models and discouraged competition and innovation
21 in the way that phones are being offered.

22 And so we think that the less
23 restrictions that are imposed on the exemption
24 now, the more it allows for the market to evolve
25 competitively and for there to be more choices for

1 consumers.

2 MS. CHARLESWORTH: Okay. Thank you.

3 Okay. Mr. Riley?

4 MR. RILEY: I have a question for
5 Consumers Union.

6 Mr. Slover, earlier you stated that you
7 advocated before Congress to draft an exemption
8 that did not include that "used" language. Yet
9 Congress, when they introduced the Unlocking
10 Consumer Choice in Wireless Competition Act, did
11 revert to the earlier exemption that did have that
12 "used" language.

13 How are we to treat that? Is that
14 Congress's intent, or do you have some other
15 explanation as to why they rejected your advocacy
16 on that issue?

17 MR. SLOVER: Well, my familiarity -- and
18 I was working pretty closely with the people on
19 both the House and the Senate side -- but what
20 they wanted to do was to reinstate the 2010
21 exemption as it was. And they were loathe to step
22 into the position of dictating changes,
23 particularly for an interim period.

24 The one exception that they made was
25 owner of the device versus the owner of the copy

1 of the software.

2 So I don't think it's a pronouncement
3 necessarily that it should be that way because
4 they left it open to the Librarian to decide
5 whether to extend the exemption, you know, in the
6 next triennial proceeding rather than dictating
7 that it should be.

8 MS. CHARLESWORTH: Okay. Thank you.

9 We all happy?

10 So do we get out of school early? Yes.

11 Thank you, everyone, for attending and
12 commenting on the unlocking exemptions.

13 We're going to wrap up for today. For
14 those of you who come back tomorrow, I think we
15 start again at 9:00 a.m. Is that correct? And
16 tomorrow with proposed class 1, which is
17 audiovisual work.

18 So thank you again, and we look forward
19 to seeing some of you tomorrow.

20 (Whereupon, at 2:46 p.m., the 1201
21 Rulemaking Process Public
22 Roundtable was concluded.)

23

24

25

1 CERTIFICATE OF NOTARY PUBLIC

2 I, CHRISTINE ALLEN, the officer before whom the
3 foregoing deposition was taken, do hereby certify
4 that the witness whose testimony appears in the
5 foregoing deposition was duly sworn by me; that the
6 testimony of said witness was recorded by me and
7 thereafter reduced to typewriting under my
8 direction; that said deposition is a true record
9 of the testimony given by said witness; that I am
10 neither counsel for, related to, nor employed by
11 any of the parties to the action in which this
12 deposition was taken; and, further, that I am not
13 a relative or employee of any counsel or attorney
14 employed by the parties hereto, nor financially or
15 otherwise interested in the outcome of this
16 action.



Christine E. Allen

19 CHRISTINE ALLEN
20 Notary Public in and for the
DISTRICT OF COLUMBIA

21
22 My commission expires:
23 Notary Registration No.:

24
25

1 CERTIFICATE OF TRANSCRIBER

2 I, JANE MOLARO, do hereby certify that this
3 transcript was prepared from audio to the best
4 of my ability. I am neither counsel for, nor party
5 to this action nor am I interested in the outcome
6 of this action.

7

8

9

10

11

12

13

14

15

16

17

18

June 5, 2015

JANE MOLARO

19

20

21

22

23

24

25

<hr/> <p style="text-align: center;">\$</p> <hr/> <p>\$250,000 56:22</p> <p>\$700 223:11</p> <hr/> <p style="text-align: center;">1</p> <hr/> <p>1 261:16</p> <p>1:45 206:1,5,8</p> <p>10 7:13,14 53:23,24 54:2 73:4 151:13 156:1 185:16 248:20</p> <p>1030 121:23 145:10</p> <p>11 123:17,21 206:6 208:13 238:8</p> <p>11:15 124:10</p> <p>11:20 124:10</p> <p>110 96:21</p> <p>11-12 3:4</p> <p>117 213:7,12 245:14</p> <p>12 96:19 156:2,4 173:15 195:7,21 206:6 208:13 248:21</p> <p>1201 1:6 4:6 12:19,24 14:17 18:9 20:13 21:20,22 24:14,25 37:13,17 38:4,10,24 51:3,20 71:8 95:15 113:2 139:22 141:10 146:5 191:6,21 206:13 223:21 229:2 232:6 239:6 248:17 261:20</p> <p>1201(a) 119:7</p> <p>1201(f) 14:20 15:18</p>	<p>1201(g) 14:19 15:17</p> <p>1201(i) 70:6 92:17</p> <p>1201(j) 13:14 14:18,25 15:16 42:9,16 76:21 86:25 88:5 92:18 101:1,19 102:12 104:2,8 105:1,19 107:14 109:20 111:16 112:21 113:16 119:14 121:19 122:8,12 129:24</p> <p>1201's 23:13</p> <p>13 63:9</p> <p>14 122:2</p> <p>1600 238:14</p> <p>18 121:23</p> <p>1853 50:1</p> <p>1990 91:9</p> <p>1991 90:20</p> <p>1994 72:11 92:5</p> <p>1995 91:10</p> <p>1996 49:14</p> <hr/> <p style="text-align: center;">2</p> <hr/> <p>2 60:1</p> <p>2:46 261:20</p> <p>20 42:19 46:21 48:3,25 49:12 127:4 175:1</p> <p>200 81:15 83:18</p> <p>2003 73:6</p> <p>2004 16:16,17 72:17</p> <p>2005 72:17</p> <p>2006 16:8 21:17 211:21</p> <p>2007 161:3</p> <p>2007-2008 72:15</p>	<p>2008 72:14</p> <p>2009 21:13,18 23:3</p> <p>2010 16:8 23:12,25 25:21 27:8 211:21 247:4 260:20</p> <p>2011 75:6</p> <p>2012 25:17 211:22</p> <p>2014 245:5</p> <p>2015 1:7 263:18</p> <p>206 3:5</p> <p>22 134:23</p> <p>25 3:3 35:9,13 83:14 100:19 124:15,18 127:11,18 128:1</p> <p>26 1:7</p> <p>28 63:8</p> <p>29th 53:21</p> <hr/> <p style="text-align: center;">3</p> <hr/> <p>3 59:25</p> <p>30 62:3 133:23</p> <p>30-page 196:11</p> <p>35 122:1</p> <hr/> <p style="text-align: center;">4</p> <hr/> <p>4 3:3</p> <hr/> <p style="text-align: center;">5</p> <hr/> <p>5 99:2 178:17 218:23,25 219:2 226:22 227:2 263:18</p> <p>5,000 230:6</p> <p>50 83:12 189:21</p> <p>5S 226:25 227:1,4,12</p> <hr/> <p style="text-align: center;">6</p> <hr/> <p>6 218:24,25 219:3</p>	<p>226:23</p> <p>60 197:9 217:21</p> <p>61 63:2,8,16</p> <hr/> <p style="text-align: center;">9</p> <hr/> <p>9:00 261:15</p> <p>90 185:15</p> <p>90-day 88:12 93:5</p> <hr/> <p style="text-align: center;">A</p> <hr/> <p>a.m 261:15</p> <p>Aaron 209:9</p> <p>abiding 24:18</p> <p>ability 44:21 54:17 59:13 61:17 70:5 90:3 105:5 115:1 127:9 135:12 152:21 175:6 231:10 263:4</p> <p>able 20:4 27:23 31:20 32:16 40:24 41:1 42:16 56:18 58:25 62:6 74:16,18 75:2 76:16 78:9,22 79:1 92:11 106:16 107:24 108:18 114:20 120:13 147:3 153:12 154:19 166:1,4 176:4 183:2 186:10 195:18 197:18 212:14 220:8 224:7 233:11,16 234:1,24 236:6 239:4 244:10 250:22,25</p> <p>absence 24:13 191:3</p> <p>absolutely 17:6 22:13 42:17 85:1 95:24 117:25 132:20 149:14 152:9 184:25</p>
---	---	--	---

234:19 237:22 absurd 140:25 abuse 120:9 203:21 abused 44:23 abusing 255:21 academia 10:5 71:25 academic 32:9 46:25 47:2,15,24 51:1 78:14 79:3 124:24 159:18 160:20 172:11 185:23 205:14 academics 48:2 89:7 134:25 160:11 accept 123:16 159:13,15 access 34:8 41:4 43:11 76:2 135:24 136:7,19 137:17 140:2 147:19 156:7 161:12 212:20 230:10 accessing 117:18,19 139:12 140:4,5 240:7 accidental 107:9 according 120:23 144:20 accordingly 22:8 230:20 account 227:7 accurate 41:22 achieve 151:21 239:3 acknowledge 118:3 acknowledged 23:12 88:3	acquire 238:18 244:4 acquired 242:6 249:6 253:16 acquires 253:22 across 44:11 68:21 69:5 107:10 158:9 161:9 184:11 185:19 230:4 act 30:15 45:24 57:21 87:21 99:3 110:7 117:17,19 120:9 122:9,10 145:9 148:21 189:13 190:4 191:23 193:14 205:1,9 206:14 213:9 245:4,8,16,20 246:1,3,8,16 247:1,7 260:10 acting 24:12 109:7 204:22 action 12:18 46:4 195:19 262:11,16 263:5,6 actions 41:21 179:23 189:21 activate 221:12 225:21,25 257:7,9 activated 217:10 219:9 222:21 223:8 225:24 242:7 249:6,16 257:7,8,9 259:15 activating 221:16,23 active 11:24 139:4 actively 44:24 47:17 130:21 activities 16:22 55:5 113:5,14	130:14 activity 106:20 247:5 actor 38:25 actors 125:18 128:25 129:17 171:6 180:17 actual 147:20 170:21 173:24 195:18 200:13 218:13 actually 14:16 15:14 17:22 18:22 21:12 37:8 40:9,12 41:6 43:9 44:18 45:1,22 48:5 49:8 56:1,13 81:1,5,8 92:9 95:20 100:1 116:13 132:5 155:6 156:12 159:11,20 162:19 176:10 183:25 184:24 192:11 205:3 222:7 249:23 250:22 257:6 adaptation 213:5 add 17:22 49:13 61:23 80:23 82:7 94:7 146:11 150:17 193:10,11 208:8,10 244:17 247:13 added 28:4 addendum 153:25 addition 77:22 94:20 142:4 170:10 229:16 231:13 additional 15:25 55:20 59:4 83:16 122:2 123:4,5,24 166:24 205:18	208:10 231:23 254:12 address 71:10 99:23 122:19 130:4,8 133:3,20 138:10 152:18 156:10 164:14 169:23 170:2 172:15 216:6 227:21 228:2 243:12 248:17 249:14 254:25 addressed 137:11 145:14 162:7 164:8 165:12 addresses 163:23 202:8 241:3 addressing 100:3 157:3 200:5 203:22 adds 213:19 adequate 151:25 adequately 98:14 adhered 233:12 adhering 98:16 administration 126:6,18 129:14 admit 11:12 ado 7:17 adopt 88:10 adopts 256:13 adults 96:22 advance 56:12,14 80:2 89:23 124:25 162:9 advantage 38:4 50:9 224:3 adversaries 177:14 adversary 175:17 adverse 119:9,11 230:17
--	---	---	---

<p>adversely 45:10</p> <p>advertised 132:14</p> <p>advice 18:23 76:22</p> <p>advise 118:2</p> <p>advised 18:2</p> <p>adviser 189:16</p> <p>advising 17:14 171:4</p> <p>Advisor 5:4 207:4</p> <p>advisories 63:11</p> <p>advocacy 210:17 260:15</p> <p>advocate 128:24 241:8</p> <p>advocated 260:7</p> <p>advocates 150:19</p> <p>advocating 86:24 87:3 89:25 120:10 224:22 241:12</p> <p>advocation 84:7</p> <p>Affairs 209:22</p> <p>affect 95:15 154:25 161:11</p> <p>affected 64:1 81:12,16 83:7 154:25 255:9</p> <p>affecting 47:11</p> <p>affects 114:21</p> <p>affidavit 145:8</p> <p>affiliated 33:24</p> <p>affiliation 7:20 209:3</p> <p>affirmative 53:4</p> <p>affirmatively 201:11</p> <p>affirmed 23:7 245:21</p> <p>afford 13:5</p> <p>affordable 213:20</p>	<p>affording 128:25</p> <p>afield 84:12</p> <p>afoul 37:25 76:10 109:12</p> <p>afternoon 209:8,19,23 210:16 244:22</p> <p>afterwards 254:25</p> <p>against 24:4 42:2 55:1 61:16 74:6 81:2 99:15,16 103:24 127:1 151:9 179:24 185:5 232:24</p> <p>age 43:6</p> <p>agencies 37:10 122:24</p> <p>agency 159:16 189:19 192:22 193:17,20</p> <p>agenda 26:11</p> <p>agent 231:16</p> <p>aggressively 158:16</p> <p>ago 11:3,4 17:2 34:14 36:18 38:9 48:2,4,7,25 49:13 127:4 160:4</p> <p>agreed 221:1</p> <p>agreement 207:19 220:17</p> <p>agreements 120:24</p> <p>ahead 13:13 19:11 109:23 214:6 216:12 249:25</p> <p>aid 186:13</p> <p>aim 89:9,14,15</p> <p>aimed 126:9 142:8</p> <p>air 115:16 134:3 187:7</p>	<p>196:9,13,14</p> <p>airline 145:4</p> <p>airplane 115:16 140:17,24 141:7 146:18 147:1</p> <p>airplanes 140:16 144:12,16,18</p> <p>alert 44:5 168:17</p> <p>Alex 21:14</p> <p>allegedly 140:14 146:25</p> <p>Allen 1:16 262:2,19</p> <p>alleviating 116:8</p> <p>Alliance 9:13</p> <p>allow 14:2 22:7 38:14 43:10 76:8 106:11,20 110:22 114:4 115:13,20 162:9 185:6 210:19 216:4 231:9,16 249:4</p> <p>allowed 41:6 73:15 85:16 108:8 139:21 162:3 170:13 217:17 243:22</p> <p>allowing 30:10 35:10 41:1 94:18 100:18 162:14,18 176:6 177:12 223:6 230:21 244:23</p> <p>allows 6:17 13:24 39:15 67:10 93:13 115:14 142:18 167:20 168:19 176:9 245:17 246:1,4 259:24</p> <p>alluded 84:8</p> <p>alone 62:20 183:25 194:14</p>	<p>already 63:9 122:15 129:4 175:23 176:4,8 186:24 191:12,21 193:22 199:1 203:1 208:1 210:24 234:20 245:7 259:8</p> <p>alternative 202:7 228:9 241:11</p> <p>alternatives 213:20</p> <p>am 4:16 8:2 9:3 39:11 48:14 59:19 108:18 136:20 141:17 147:6,24 159:7 169:19 170:3,9 173:23 238:4 262:9,12 263:4,5</p> <p>amateur 32:22</p> <p>Amazon 257:14,15,16</p> <p>ambiguities 38:4,13</p> <p>ambiguity 117:20 127:12 247:10 256:16</p> <p>ambiguous 17:18 37:23</p> <p>amenable 118:3 119:18 201:22</p> <p>amended 128:2 232:6</p> <p>Amendment 23:20 85:20,24 86:23 87:1,8,16 92:21,22,24</p> <p>Amendment-protected 85:11</p> <p>America 23:10</p> <p>American 96:22</p> <p>Americans 25:7</p>
---	--	--	--

45:16 96:21 America's 9:7 among 20:11 68:21 215:18 238:15 amongst 153:18 amount 131:13 amplify 5:12 amplifying 122:14 analogous 73:3 analogy 113:7,8 117:5 196:24 analysis 16:20 30:8 59:6 60:18 171:23 172:8 212:17 245:14,15 analyze 48:24 73:19 ancient 48:5 Andrea 8:24 Android 155:2,3 Andy 8:17 34:25 anecdote 142:10 Angeles 5:10 6:19 Anna 9:16 annex 55:13 announced 126:22 anonymously 43:3 answer 27:11 29:4 46:7 77:19 83:3,4 116:20 122:17 129:18 131:10 139:25 169:24 185:8 211:14 216:17 223:12 247:24 258:2,12 answered 80:6 anti 77:24 97:6 213:21	anticipated 77:7 anti- circumvention 12:18 96:2 anti-trafficking 77:21 anti-virus 174:3 anybody 121:6 anymore 20:8 anyone 138:3 150:22 200:12 219:6 anything 13:21 22:13 26:15 92:9 94:7 133:21 145:5 160:17 193:10 199:2 237:25 244:16,20 255:24 anyway 19:6,18 88:25 141:8 226:4 anywhere 187:7 200:1 apologized 45:3 Apparently 144:19 appear 94:25 246:15 appeared 21:16 appearing 238:7 appears 242:3 262:4 Apple 81:18 applicable 121:22 128:12 133:8 184:14 203:4 application 11:19 applications 22:25 54:11 71:21 73:7 114:15,23 applied 10:2 13:17	17:19 113:9 applies 15:17,18 139:15 182:18 256:15 apply 15:20 69:5 76:21 85:13 113:8 133:9 136:10 139:10 160:10 197:20 231:3 245:22 259:4 applying 101:19 241:2 259:1 appointment 196:18 apposite 190:6 appreciate 150:8 205:13 appreciative 116:13 approach 65:5 68:19,20 69:16 70:15 77:11 82:25 93:9 158:19 203:22 approaches 81:24 172:2 appropriate 30:6 67:13 69:14 101:11 approved 161:17 211:21 April 53:21 arbitrage 240:9 arbitrarily 213:18 area 10:2 27:19 30:15 88:22,24 122:23 136:17 147:23 160:15 162:5 areas 5:13,17,18 58:11 113:5 188:19 204:20 207:14	aren't 25:5 131:24 183:23 184:3 185:11 188:16 201:6 203:25 arguably 48:18 120:23 argue 13:5 15:16 17:6,8,9,10 127:11 174:17 argued 15:1 argument 15:13 52:10 86:20 88:3 92:22 117:3,11,14 176:13 192:13 arise 51:3 arises 51:19 arising 68:19 71:7 arm 210:17 arms 24:22 arm's 237:14 arrangement 219:22 241:21 array 22:19,21 186:20 217:24 arrayed 215:18 arrow 40:12 article 54:9 92:23 168:11,17 173:14 196:10,11 artificial 62:13 aside 60:9 140:20 aspect 125:12 aspects 141:16 asserting 192:2 assess 59:13 237:18 assessed 39:13 67:8 assignments 49:9
--	---	--	--

assist 97:1 99:9	63:2 77:13	125:22	background 51:4
assistance 20:19 44:6 67:9 231:15	attempting 21:24 188:6	auto 158:23 196:6	backward 29:21
Assistant 4:22 5:1 206:22 207:1	attempts 23:18 65:21	automobile 133:20,25 134:16,20 135:12 152:8 194:2	bad 24:22 87:10 91:7,15 97:24 125:4,18 127:2 128:25 129:17 148:14 157:25 159:12 164:12 166:17 171:23,24 176:7,10 180:17
assisting 59:5 189:14	attend 135:2	automobiles 133:21 194:2	bad-hat 52:9
associate 209:21 230:24	attending 261:11	automotive 11:8 192:18	bag 196:9
associated 97:21	attention 94:16 178:9		bags 134:3 196:13,14
association 93:6 209:18 211:5 229:23 230:1,2 238:13	attorney 5:3,6 51:5 54:5,19,24 56:25 57:19 89:5 207:3,6 209:16 262:13	available 63:4 97:16 175:23 222:25 230:12 238:25 248:9 256:23	balance 30:7 49:23 52:20 82:2 83:25 126:25 176:18
assuaging 143:4	attorney-client 77:1	avenue 217:5	balances 127:8
assume 75:1 104:6,7 105:17 184:20 229:1 258:12	attorneys 18:3	avenues 229:1	balancing 29:15
assuming 191:8 227:22	audience 5:8	average 133:23 175:8 228:12	bank 101:20 102:21 105:23 106:14 108:14,15 116:23 117:1,2 120:6,7,12
assurance 67:12,16 149:19	audio 39:15,22,25 40:7 43:12 263:3	avoid 65:25 66:6 81:11 128:16 160:17 236:25 247:9	banking 102:16
AT&T 46:22 215:15 221:13 222:20 225:16,19,21,24 227:10 228:16 233:14	audiovisual 261:17	avoided 24:12	barrier 223:2
atop 23:1	audits 99:10	avoiding 79:9 146:14	bars 148:12
attached 26:1 236:1	Australia 78:4	award 200:25	based 12:18 125:14 155:10 202:2 205:19 222:16
attack 48:25 49:3,8 90:23 194:7	authentication 198:16	awards 44:19 200:21	Bash 36:14
attackers 51:8 96:11,14 97:4	authored 49:1	aware 35:7 91:6,25 163:8 259:13	basically 6:5 68:2,5 78:7 88:10 107:14 112:17 143:17 214:21 227:3
Attacking 120:7	authorities 162:23,25 163:3	away 46:3 112:18 144:24 195:24 196:4 225:19	basis 16:7 54:25 56:18 57:9,21 66:4 67:17 68:18 80:6 93:14
attempt 51:12 54:8 63:21 65:3 77:5 154:11 199:21	authorization 34:16 42:3 101:5,11 103:13 105:11,24 106:4,5,7,12,21 107:5,15,23 109:4,14 110:18,23 111:1,6,9,13,18 125:13 128:5	awry 59:7 60:23	
attempted 54:13	authorize 132:5	<hr/> B <hr/>	
	authorized 34:5,6 161:14,15,16	baby 40:15	
	authorizing	back-and 70:13	
		back-and-forth 11:18 162:1	

164:20 batteries 194:22 became 10:6 become 22:20 23:3 81:4 becomes 81:22 146:23 176:19 becoming 45:16 bed 77:9 beforehand 17:14 19:2 111:10 begin 20:10 124:7 133:17 beginning 111:1 behalf 14:14 35:5,8 94:19 178:2,10 241:9 258:18 behave 64:11 behavior 75:14 145:15,17 229:5 241:12 behind 86:17 132:11 250:12 belabor 67:19 believe 11:16 44:21 56:10 57:17 70:19 92:16 125:21 128:1,18 141:1 188:10 200:11 211:17 214:9 218:24 233:20,22 245:9,15 246:1 247:6,7 believed 11:16 65:16 believes 230:14 231:25 bell 46:22 72:1 249:21 Bellovin 8:22	46:16,17,19 61:23,25 71:24 90:17,18 116:3 119:25 120:1 146:7,8 148:1 158:2 159:5,6 161:2 166:6 192:15 193:6,9,11 204:11,12 Bellovin's 195:13 benchmark 30:20 beneficial 158:14 benefit 62:21 67:11 90:5 139:24 140:1 151:25 190:15 benefits 93:11 162:17 177:12 238:22 239:3 245:10 246:12 best 7:2 45:13 63:6 100:4 118:14 126:16 128:20 158:23 163:20 187:3,15 198:21 204:18 205:7 263:3 bet 117:13 better 13:15 29:5 33:2 37:11 98:1 102:11 149:9 172:18 187:9 199:12 211:13 227:1 beyond 81:20 133:21 bigger 222:8 big-tech 69:2 bill 246:10,19 bills 126:14 bill's 246:20 binary 48:11 bipartisan 211:24	birth 41:7 bit 6:1 11:13 17:23 28:18 58:11 72:25 76:20 82:22 95:1 101:15 114:12 132:3 142:24 143:16 155:1 160:25 162:5 170:23 174:14 175:14 190:10 207:14 245:8 black 129:5 135:3 175:19,24 180:12,23 181:9 190:16 192:4 240:16 241:10 black-market 181:21 Blake 8:14 13:20 Blaze 9:3 70:23 71:13,14 76:24 77:24 78:17 79:20,22 80:1,4 84:8 89:1,3,4 90:10,14 93:22 94:6 150:15,16 151:14 160:23,24 161:15,24 162:25 163:2,8 181:15,16 183:14,17 184:19,25 185:25 186:2 193:22 204:16 blind 233:7 block 159:10,16 160:7,8,17 blog 174:15,21 blueprint 15:19 bluster 153:11 BMW 164:21 165:19 166:23 167:1 board 69:6 93:8	178:7 boards 147:19 bodies 152:17 Boeing's 147:3 bogus 193:18 bolsters 97:19 bono 18:4 20:15 book 49:1,12,14,19,25 50:1 books 148:18 247:4 bookstore 247:3 bother 47:6 bothered 92:10 bottom 59:8 bought 76:2,3 102:2 117:2,12 174:23 249:15 Boulder 35:2 bounds 109:10 bounty 53:1 200:21,25 box 120:25 brain 6:24 brakes 183:3,7 184:5 braking 134:3 brand-new 88:2 brave 40:3 breach 35:25 94:24 97:22 138:19,20 breaches 96:23,24 break 43:19 124:6 138:19 148:23 226:18 252:23 breaking 146:14 breathing 24:19 Brian 209:23
---	--	---	---

<p>244:25</p> <p>bridge 233:18</p> <p>brief 4:3 5:23 7:22 86:2 92:13 158:3 180:21 181:17 207:16 245:4</p> <p>briefed 85:23 88:4</p> <p>briefing 86:3</p> <p>briefly 149:6 173:12 177:25 209:2 211:16</p> <p>bright-line 181:19</p> <p>bring 74:4 154:16 179:23 233:24</p> <p>bringing 158:19 200:23</p> <p>brings 200:22</p> <p>broad 6:7 21:19 24:5 28:4 31:13 75:14 116:7 129:8 135:10 136:10 182:23</p> <p>broader 26:20 127:20 129:12 137:1,16 181:6</p> <p>broadest 118:1</p> <p>broadly 71:22 128:22 152:4 191:5</p> <p>broken 20:7 191:12</p> <p>brokers 238:14</p> <p>brought 99:15 117:5 179:20 201:2 253:11</p> <p>BSA 9:13 125:6,8,11 126:13 135:22 157:11</p> <p>BSA-member 130:19</p> <p>BSA's 110:4</p>	<p>buck 188:4</p> <p>buffer 47:5</p> <p>bug 36:14 53:1 175:16 200:21,25</p> <p>build 71:20 77:8,9 79:13 133:6 186:7 233:9</p> <p>building 32:24 89:12 174:13 180:7</p> <p>built 172:5 203:25 234:20</p> <p>built-in 22:1 23:13</p> <p>bulk 222:10 225:6,7 226:9 227:21 228:7 232:24 239:5 246:1,10,12 247:6 252:15 253:5,23 256:15</p> <p>bunch 101:20 103:17 144:12</p> <p>bundle 187:2</p> <p>burden 38:23 152:14 226:5</p> <p>burdens 37:23</p> <p>business 44:22 45:9 212:7,10 213:22 241:7,16 259:19</p> <p>businesses 45:8,14 51:6</p> <p>button 40:11</p> <p>buy 101:20 103:20,22 175:1 176:3 223:10 233:5,6,14 235:5 240:1 241:6 252:22 257:15,16</p> <p>buying 157:16 167:16 168:23 213:24 222:11</p>	<p>buys 237:2,3 251:8</p> <p>by-case 164:20</p> <p>bypassed 213:1</p> <p>bypassing 12:22 13:23 14:7</p> <hr/> <p style="text-align: center;">C</p> <hr/> <p>cabin 170:12</p> <p>cabined 111:14</p> <p>cafeteria 206:3</p> <p>calculation 155:1,9</p> <p>calculus 93:23</p> <p>California 178:6</p> <p>camera 43:8,16 44:4 45:1 156:13 173:15</p> <p>candidate 34:25</p> <p>capable 172:9</p> <p>capacity 9:2 50:24 132:10</p> <p>Capital 1:17</p> <p>car 104:22 158:5,9,10,20,22 ,25 167:17 183:3,25 184:7 196:2,3,4,17 197:6,8,11 231:19</p> <p>care 24:17,24 142:7 191:22 253:20</p> <p>career 10:5,18 90:19</p> <p>careful 127:8 160:16 245:13</p> <p>carefully 5:20 118:18 208:2 247:25 249:2</p> <p>carried 128:6</p> <p>carrier 212:10</p>	<p>214:22,25 215:13 218:24 219:9 220:22 221:2 224:5,6,7 225:12,25 231:11 233:25 234:5,23 235:9 239:2 240:2,7 242:8 243:22 245:12 249:7 253:14</p> <p>carriers 155:4 209:18 211:5 214:10 215:10 222:3 223:13 229:23 230:1 233:4 237:7 240:17 250:21,25 256:24 257:2 259:13</p> <p>cars 11:9 22:22 26:7 158:4 165:4 182:25 184:2</p> <p>case 12:20 13:6 14:6 19:20 37:1 56:4 62:22 63:18,20 73:3 78:19 80:24 84:25 91:24 92:11 104:17 139:12,15 148:6 155:21 162:14 164:19 165:7 166:21 180:25 193:17 194:3 201:19</p> <p>case-by-case 80:6</p> <p>cases 10:14 34:9 64:3,4,21,22,23 65:1 78:18,19 79:10 80:7,13,23 90:25 91:5 92:7 99:1,15,18 154:12 164:17 183:19,22 184:12 185:12,14</p>
--	---	--	---

193:15,18 232:8 254:22 catastrophic 138:21 categorical 80:19 category 53:12,15 caught 48:22 212:8 cause 22:6 140:7 caused 10:20 22:15 135:24 136:18 causes 81:4 160:10 184:5 caution 84:20 CCA 229:14 230:9,14,20,25 231:25 232:9 242:18 251:17 252:8 CCA's 230:4 243:19 cell 28:10 35:20 102:8 104:22 215:24 251:8,12 252:15,16,22 center 9:10 100:16 126:15 209:11 centuries 213:17 CEO 157:1 CERT 63:14 91:2 certain 25:12 38:1 45:24 81:20 146:12 159:24 161:24 165:1 166:15 176:6,14 212:9 217:17 certainly 43:5 65:13 78:18 79:8 80:7 81:16 98:3 121:5 130:17 132:12 135:7 136:22 137:7 139:19 148:7	150:20 151:16 157:10 158:14 159:7 164:16 178:2,8,16 183:18 242:1,3 243:11 certainty 15:2 17:21 23:16 25:5 28:7,15,21 CERTIFICATE 262:1 263:1 certify 262:3 263:2 CFAA 122:9 128:12 139:10 146:17 147:11 148:2,21,25 chain 105:25 106:6 156:10 chairing 201:10 challenge 65:15 challenges 203:23 chance 83:24 175:18 254:11 255:10 change 45:2 56:3,9 90:21 220:2,6 changed 214:18 215:4 changes 162:16 260:22 changing 187:1 channel 57:25 58:1 59:4,10,11 62:13 67:13 69:17,19 channels 59:9 156:21 chaperoned 210:12 chaperoning 210:7	chapter 49:2,24 characterize 124:18 Charlesworth 2:2 4:2,8 5:7 8:5,10 9:20 12:3,8,10 13:9,12,14 14:11 16:11,17 17:11,24 18:15,22 19:3,5,8,11,14,1 6 20:25 29:6,9,24 30:12,17 32:3,6 33:5 34:4,17 36:16 37:2 39:7,16 40:1,5,15,19 43:14,18 46:8,16 50:15,19 51:21 53:22 63:19,25 64:3,17 65:7,24 66:11,21 67:18 68:25 69:21 70:1,22 71:12 82:14,24 85:23 86:5 87:2 88:1 89:3 90:7,11,15 92:12 94:4 100:13 112:9,16 118:6,13,16,23 119:24 121:15 122:25 123:3,7,10,12,15 ,19,23 124:1,14 129:20 130:2 131:6 132:2,15 133:14 135:18 136:14,24 137:15,19 140:12 141:21 142:1,15 143:3 144:19 146:6 147:22 149:4,16,24 150:7 151:13 152:5 153:1 154:7 155:13,24 157:6,9 158:1	159:5 160:23 161:13,22 162:21 163:1,5,11 164:4,7 165:13,17 166:11 167:13,16 168:10 169:5,7,10,18,20 ,25 170:22 171:20 172:17 173:6 174:9,12 176:12 177:16 178:23 179:15,18 180:19 181:13 183:5,16 184:16,20 185:21 186:1,16 187:6,13,18 188:11,15,20 190:8,21,23 191:2,6,11,18,20 ,25 192:7,10 193:6 195:6 196:21,25 197:3 198:1,5,18 201:5,8,25 202:9,25 203:9 204:2,10 205:10 206:10,15 207:8 209:1,13 210:11 218:6,20 219:11,18 220:12,15,18,25 221:4,10 222:5 223:4,9 224:13 225:3,13 227:17,20 228:14 229:11,19 232:21 237:25 238:3,5 239:18,24 240:6 241:22 242:5,11,14,23 243:1,13 244:14,19 248:3,15,23
--	---	---	--

<p>249:19,25 253:8 254:14,20 256:6,18 258:2,5,13,22 259:11 260:2 261:8 Charlie 33:24 192:17 checks 127:8 Cheney 2:11 5:5 46:9,11,15 203:10 207:5 256:20,21 257:18,22 258:3,4 chief 193:12 child 39:23,24 40:6,10,12,22 41:5,7,8 43:4 151:19 167:21 168:20 169:3 children 42:24 44:24 children's 39:14 44:18 child's 41:2 chill 27:22 chilled 24:13 75:6 119:20 chilling 21:23 23:2 113:4,22 116:8 121:7 127:13 130:13,18 134:15,18 152:10 160:11 203:17 204:24 chime 84:2 116:5 142:3 163:14 195:12 202:10 chip 11:6 12:4,6,7 16:15 72:13 Choe 2:3 4:19,20 206:20 choice 62:17 188:14,15 189:1</p>	<p>192:17 230:13 232:16 257:20 259:10 260:10 choices 97:18 213:23 259:25 choose 38:17 144:5 188:3 choosing 81:8 230:25 chorus 150:17 chosen 74:12 Christian 9:12 Christine 1:16 262:2,19 circle 173:10 circling 179:13 circuit 147:19 circuits 203:21 circular 142:16 circumstance 107:1 circumstances 31:3 48:19 80:20 105:21 195:17 197:19 circumvent 14:2 191:7 circumvented 134:8 150:4 191:16,21 circumventing 24:23 147:15,16 circumvention 26:12 35:10 36:19 37:1 42:2 87:24 97:7 109:13 127:7 128:2,6 145:7 148:12 191:11 212:9 216:5 232:3 Cisco 44:20 102:2</p>	<p>citation 145:8,10 cited 95:19 99:19 citizens 39:3 city 227:5 civil 216:23 claim 75:1 166:14 237:10 claimed 74:11 claims 74:7 248:11,21 clarification 70:20 137:20 clarified 253:19 clarify 5:12 92:15 244:10 253:10 258:6 clarity 15:25 25:5 93:12 117:22 118:5 119:2 class 3:3,4 6:7 35:9,13 80:7 100:19 121:2 124:15,18 125:12 127:11,18 128:1 129:10 133:19 134:23 136:9 238:8 261:16 classes 47:3 206:6 208:13 classification 127:15 classroom 31:19 32:7,20 33:4,6 clause 246:10,21 cleaner 255:25 clear 15:25 16:6 24:19 25:9,12 31:1 45:6 53:6 58:5 79:12 80:14 85:7 87:4 100:6 119:20 122:22 202:18 205:15</p>	<p>212:23 224:14 237:12,16 239:6,15 246:25 253:15,18 256:15 258:8 clearly 63:22 88:15,21 139:25 161:7 229:3 click 120:24 client 35:5 clients 10:13 Clinic 8:15,18 35:4 209:25 210:4,6 245:2 248:5 Clipper 72:13 clone 54:17 close 10:9 24:15 205:11 closed 120:17 156:12 201:15,18 202:8 closely 91:16 212:4 260:18 closer 237:1 closest 187:16 club 205:4 CNN 96:18 co 48:25 code 48:11,13 147:9,19 148:9,17 149:1 200:17 codify 177:3 collaborating 125:9 collateral 22:6 144:9 colleague 71:24 78:3 118:9 141:16 247:23 colleagues 4:10,17</p>
---	--	--	--

10:24 11:4 21:19 22:12 23:9 25:4 34:22 36:3 198:6 206:18 243:6 colleague's 64:8 collective 46:1,4 colloquy 244:8 253:11 color 142:11 Colorado 8:16,19 35:2,5 Columbia 8:23 46:20 262:20 comes 107:10 173:22 197:7 200:12 comfort 57:11 61:4,9 93:12 94:1 186:14 comfortable 93:14 136:23 137:2,13 202:17 242:3 256:4 coming 30:5 32:16 86:7 195:8 commands 45:24 comment 14:14 36:22 46:25 95:3 122:3 123:1,10 135:25 138:25 158:3 208:11 240:11 245:15 256:9 commentary 88:7 91:12 commentators 88:22 commenters 95:18 commenting 261:12 comments 5:15,19 7:5,8 14:23 31:18 35:8 60:1 88:25 93:7	121:24 125:5 133:18 150:8 177:23 193:8 207:24,25 211:19 222:9 231:2 242:19 254:15 Commerce 2:11 5:6 126:21,24 207:7 commercial 10:11 20:9 33:19 145:1 247:5 commission 98:23 99:3 193:12 262:22 commit 202:15 commits 178:13 committed 178:11 Committee 232:4 committees 201:11 commodities 238:15 common 10:18 commonly 189:4 communicate 41:2 43:3 54:13 communication 39:23 40:8 45:4 164:9 communications 75:8 122:10 167:21 168:20 communities 124:25 188:12 community 32:9,22 36:8 57:12 71:3 74:18 78:14 79:4 89:8 90:25 91:6,20 92:1,10 111:5 125:10 130:21 149:14,22	158:15 162:12 175:10 181:7,21 185:24 193:3 198:20 199:8,20 205:14 companies 10:7 51:5 52:22 53:16 62:12 63:2,8,9,16 64:1,10 66:1,16 69:3,7 81:13,15,17 94:3 100:1,2 121:13 130:19 131:15 132:2,9,21 153:20 154:2,12 155:12 157:15,16 158:5 179:2,9,24 189:23 200:10 238:17 company 1:17 10:8 41:16 53:9,12 56:6,18 58:21 59:13 60:6 62:10 64:20 65:11,17 67:22 69:18 99:21,22 103:9 117:13 148:8 154:18 156:19 157:1 158:25 168:15 172:1,4,15 174:3 189:11,14 191:17 200:18,20 company's 66:20 compatible 87:15 compensate 53:2 competent 194:10 competition 210:22 239:1 259:20 260:10 competitive 209:18 211:5 213:22 229:23 230:1,3	competitively 259:25 complaint 99:20 129:25 completion 41:9 complex 131:20 157:23 177:2 complexities 18:12 84:14,19 176:25 compliance 134:10 146:13 compliant 200:11 complicated 84:4 85:18 145:20 171:11 comply 13:7 complying 256:4 component 12:21 37:10 components 35:19 compounding 122:13 comprehensible 48:13 comprise 22:21 compromise 182:3 232:11 243:19 compute 23:11 computer 9:4,25 10:2,9 11:5 15:9 26:24 35:1 46:20 47:7 71:18 91:2 101:6,17,23,24 102:4,9 104:13 105:3,7,12 108:5 111:20 116:24,25 117:8,16,18 120:6,8 148:13 158:20 170:25 171:1 203:20 Computers 35:19 computing 35:25
---	--	--	--

<p>37:11 38:16 71:23 CON 135:4 158:20 concealed 22:16 concede 143:24 166:22 169:8,11 241:2 conceive 111:4 concept 242:22 concern 43:5 56:19 71:2,7 77:20 88:21 111:23 115:20 116:21 117:4 126:24 129:3 132:17,21 133:3,4,12,13 135:10 137:6 138:15,18 146:21,23 160:14,15 166:12 176:16 198:10 204:25 223:18 225:4 226:10 227:23,25 228:1,4,6,15 233:8 235:12,15 241:1 244:12 248:14 253:21 concerned 31:15 33:14 47:3 71:22 72:6 75:11 76:4 95:15 103:12 146:14 152:12 159:1,3 183:4 194:15 233:22 235:16,20 246:11 252:20 concerning 55:6 198:22 232:2 concerns 28:6 30:25 31:8 42:20 69:1 71:10 74:19 85:14 88:22 92:17 93:24 95:1,19 134:9</p>	<p>135:16 144:9 145:12,23 152:18 172:15 180:7,18 205:3 228:22,24 235:2 239:7,13 241:4 245:10 251:3,4 252:9 concluded 261:22 conclusion 77:2 90:8 119:13,17 conclusions 116:11 118:8 concurrent 128:23 concurrently 80:3 condemns 150:17 conditions 159:24 214:21 216:18 256:2 condone 239:17 conduct 20:9 57:8 113:16 115:5 149:12,15,23 161:5 199:9 conducted 11:11 47:15 50:8 114:10 conducting 72:20 90:1 96:15 conference 135:4 conferences 158:21 173:19,20 confidence 19:22 confident 216:22 confidential 44:11 confines 107:22 111:24 confirmed 246:7 Congress 1:4,8 30:15,18 37:16 69:23 70:4,6,15,16</p>	<p>84:12 86:8,10,22 87:4,14 88:15,21 95:14 113:12 122:24 126:6,8 127:4,6,22 129:13 141:12 170:23 171:9,11 211:23 212:4,5 213:9 224:17,22 231:13 233:23 245:8 246:25 247:4 260:7,9 congressional 111:25 126:15 127:24 129:11,23 137:11 143:14 Congress's 23:14 260:14 connect 230:15,22 231:5 257:6 connected 44:18 102:17 103:1 108:6 210:20 212:25 232:16 connection 54:7 223:25 253:13 cons 224:2 consensus 204:13 205:6 211:8 consent 110:12 consequence 51:19 113:4 consequences 24:25 25:10 126:5,18 128:17 152:11 consider 85:21 86:8 87:6 143:12 144:3 150:14 199:18 212:1 255:10 259:6 considerable 12:13 consideration</p>	<p>21:8 74:4 151:25 164:18 considerations 70:18 78:9 97:11 127:5 considered 35:17 68:15 70:12,15,16 160:9 considering 51:10 71:15 97:9 98:4 126:8,19,22 152:2 consistent 71:6 127:24 128:15 129:10 143:14 153:20 232:1 consistently 84:3 console 52:12,13 consonant 70:19 constituencies 68:22 constitute 118:24 constitutes 99:1 102:9 constitutionally 87:24 88:5 constrained 224:11 constraint 130:6 Construction 50:2 construed 249:3 consultancy 54:7 56:24 consultant 39:11 consumer 22:21 94:21 95:1,12,16,19 96:4,9 98:4,6 137:25 165:21 166:22 167:25 168:1,9 170:4 171:21 172:12</p>
---	--	--	--

174:5 175:8 189:25 193:16 197:23 210:17 212:15 213:22 217:1 222:20 224:1,3 225:9 227:18 228:12 231:16 241:15 253:22 254:6 255:18 256:3 257:22 259:9 260:10 consumers 23:21 51:8,14 70:10 97:5,9,18 98:17,19 121:13 151:8 153:21 154:25 155:6,7,8,11 163:17 164:2,8,14 165:1,9,23,25 166:20 167:12 168:22 169:14 170:7 172:24,25 173:24 174:17,20 175:5 189:24 195:1,18 197:19 210:19 213:13,21,23 214:24 217:13 220:7 222:25 226:17 230:18,21 231:9 238:15,23,25 247:18 254:7 255:9 260:1 consumer's 216:20 Consumers 209:11,15 210:16 228:3 260:5 contact 54:9 62:9 63:2,4,6 64:24 65:13,22 67:22 68:13 69:13,14 70:16 78:23,24	94:3 188:6 189:11 contacted 41:10 44:5 contacting 63:14 93:14,19 contain 74:3 127:21 243:19 contained 148:17 contemplate 199:21 contemplated 120:5 contemplating 70:4 contest 48:17,18 context 28:10 32:15 58:7 92:18 95:2,11,18 96:4 98:11 142:20 146:1 152:19 204:22 contexts 201:16 contingent 187:11 continue 37:5 40:20 44:22 45:9 113:14 156:14 163:24 169:3 199:16 221:5 228:12 232:13 244:15 248:24 continuing 21:7 71:10 contours 145:20 contract 160:19 161:19 217:15,18 218:8,9,11 219:2,4 220:12,16,21,24 221:25 222:21 223:19,25 224:4 225:11,17 226:19 233:3,6,13,15	234:10,12,18 236:19 237:5,10,19,20 242:25 243:1,21 244:7 252:21,24 253:13 contracted 161:20 contracts 219:20 222:24 232:20 contractual 162:1 221:8 241:13,20 contradictory 24:3 contrary 90:2 134:19 contravene 86:22,25 contravenes 87:8 contribute 6:25 contribution 47:9 contributions 5:16 32:21 control 43:11 45:20 133:24 134:2 135:12 140:3 160:10,13 197:8 232:14 controls 42:3 126:23 134:3 135:24 136:7,19 137:17 148:13,14 controversy 5:17 convenient 74:14 212:9 conversation 7:1 42:13 51:13 52:2,3 190:12 208:8 conversations 41:19 42:12 53:8 77:1 188:8 convert 48:11	73:16 convicted 91:17 convince 156:8 188:9 coordinate 205:7 cope 49:18 copied 212:24 copies 49:20 121:2 140:5 245:19,23 copy 49:14 53:20 93:2 121:2,8 146:24 147:3 213:11 260:25 copying 85:4 147:8 213:2,5 copyright 1:5 2:2,4,5,7,8,10 4:9,21 16:5 17:9 27:1 31:5,6,12 34:21 35:13 38:21 49:21 50:1 57:21 67:25 69:13,19 84:10 89:13 94:21 95:6,8 112:17 128:11 136:5 144:17 145:2,9 146:3,9,16,20,23 147:4,15,16,17 148:20 150:9 202:15 204:25 205:2 206:13,16,21 212:1,11,13,17,2 4 228:6,15,21 232:2 245:9,20 256:12 copyrightable 212:23 copyrighted 13:25 14:8 17:8 31:11 117:19 145:1,5 147:10,20 148:4 149:1,2 Copyright's 232:4
---	---	---	---

core 36:5	234:16	115:11 126:1	CyberLock
cornerstone	couple 34:14	150:18 154:4	38:11,12 54:9
213:17	91:11 119:18	161:7 180:9	55:10 57:25 73:3
corporate 46:23	179:1 214:7	critically 37:15	74:25 98:3
51:5 58:22 60:2	216:17 229:25	criticism 74:10	cybersecurity 25:7
200:5 201:16	239:20	crowdfunding	35:18 37:16
238:19	course 19:24	157:21	121:25 129:12
correct 24:9 52:6	89:18 117:3	cryptographic	178:2
69:17,19 104:8	125:3 139:15	73:7,18	cyberthreat
137:18 165:19	167:2 180:13,14	cryptography	178:19,21
218:21 258:21	186:23 191:14	10:3 71:21 73:24	
261:15	193:5	crystal 100:6	<hr/> D <hr/>
correcting 189:14	court 6:13 17:6	CTO 44:8 173:15	D.C 1:10
correction 63:15	29:10,11,20	curb 51:18	dad 237:2
correctly 50:17	117:24 208:4	cure 128:21	daily 35:19 125:21
83:1 86:11 88:14	cover 31:4 83:5	curiosity 50:10	Damle 2:6 4:24
153:9 183:8	252:15	curious 102:6	58:17 59:16,21
cost 20:21	covered 17:7	108:23 138:8	60:9,16
56:21,25 57:1	31:23 247:7	219:5 240:19	61:1,12,21,24
65:18 97:24	257:3,11,13,21,2	250:11	101:13 102:6
costly 97:24	2,24	current 27:4	103:7
cost-minded	crack 116:18	110:21 127:25	104:1,6,16,19,21
213:21	crafted 249:2	203:5 214:22	,24 105:8,15
costs 97:21	crappy 195:22	224:15,17 239:8	106:10,16,19
counsel 4:9,23,25	create 51:6 126:16	250:7	108:1,11,13,18,2
5:2 9:7,16 29:1	131:18 135:15	currently 10:4	5 109:3,16,18
54:21 55:21	creating 24:4 82:5	65:14 88:5 126:8	110:17 113:24
56:15,17 57:6	126:4,10 136:7	187:3 188:22	114:24
67:9 118:20	215:7	190:3 191:5	115:6,19,25
206:16,23,25	creation 60:2	199:13	118:11 206:24
207:2	credibility 201:17	203:16,23	214:4,7,14
209:11,15,21	credit 47:24	custodian 105:24	215:13,16
238:12	criminal 43:10	customer 114:23	216:9,12 224:14
262:10,13 263:4	44:23 160:12	customers 41:24	225:2 234:6,9,14
counsel's 54:22	188:22 216:24	44:16 45:10,14	235:1,14,18
56:15	252:3	97:13 161:17	236:2,11,16
counterbalanced	criminals 83:23	230:8	237:12,16,23
50:13	181:21	customized 83:25	242:15,25
counterintuitively	criteria 160:6	cut 67:2	243:2,8 244:8
6:23	202:6	cuts 213:18	249:21
countervailing	critical 35:17 36:6	cutting-edge	250:1,2,16,18
52:4	37:10 39:2 45:9	230:11	251:5,12,15,18,2
country 160:14	51:15 95:24		2 252:5,13
161:6 230:4	100:9 114:14,20		253:1,6
			258:5,6,15,16,24
			259:2
			Damle's 112:3

danger 151:19	163:19 165:10	delineated 58:4	design 134:14
dangerous 139:7	169:2 187:24	demand 167:23	designate 69:19
143:6 194:21	decision-making	186:9	designated 70:16
DARPA 33:23	97:12	demands 89:10	designating
37:9 135:6	declined 55:4	181:24	69:13,17
data 35:25 94:24	deemed 127:23	Democracy 9:10	designed 139:12
100:5,7 126:11	159:23 200:24	100:16	desire 232:5
227:11 228:16	deep 17:4	demonstrated	desk 60:24
data-flow 70:11	deeply 116:12	73:25	156:5,8,12,14
data-gathering	144:23 149:19	demonstrates 36:6	desperately 20:23
70:11	205:15	200:13 245:8	Despite 41:11
date 41:7 71:5	DEF 135:4 158:20	denote 76:15	44:13
Davis 54:6,13	defective 151:9	deny 95:20 246:12	detail 31:17 55:23
55:10,14,22	defend 56:18	department 2:11	165:14 166:13
day 54:5,23,24	61:17 74:6	5:6 9:4 60:25	170:14 182:12
55:15 57:19	117:25	71:19 91:3	187:1 195:20
125:10 157:2	defense 91:3	126:21 207:6	196:12
175:15 227:13	144:16 150:2	depend 46:4 106:3	detailed 14:23
230:18	defer 114:11	108:10 114:14	167:7 184:22
days 156:7 174:7	195:10 203:7	depending 14:4	185:10 254:1
175:15 176:6	deficiency 121:21	120:14 242:2	details 17:16
188:22,24	deficient 52:6	depends 15:6	41:11 43:4
deadline 131:25	define 6:8	115:3 184:25	164:10,25
deal 11:22 34:1,15	defined 111:17	deposition	172:10 174:4
49:22 51:11	defines 160:5	262:3,5,8,12	182:16 183:20
66:11 139:12	definitely 180:25	Deputy 4:24	185:6 193:4
144:8 214:24	228:4	206:24	194:16
222:2,4 224:8	definition 30:9	derive 182:16	determination
241:5	103:5 106:2	derived 15:7,10	130:12
debate 126:16	200:1 221:17	26:22 128:8	determine 40:24
129:13 246:14	222:8,16 225:23	describe 182:4	101:10 129:8
debated 141:12	226:6,8 241:23	184:8	172:12
debates 126:7	242:2,4 249:18	described 13:18	determined 41:20
decade 11:4 21:15	256:13	23:19 249:12	98:23 185:17
51:2 71:3,5	definitionally	259:6	deterred 57:15
decades 74:12	111:17	describing 16:23	develop 76:7
decide 93:17	definitions 217:9	90:23 170:19	100:2
167:22,23 179:3	degree 12:21	182:5 227:9	developed 11:20
226:25 261:4	36:25 88:16	239:25 247:24	78:5
decided 19:6 73:6	93:17 158:8	description 167:8	developer 125:16
76:18 91:14	delay 4:3 159:11	192:20	128:21 152:3
decides 168:17	delete 90:23	deserve 164:3	developing 84:18
decision 25:2			development

35:18 device 39:24 40:25 41:2,6 43:11,13 103:19,21 120:20,21 147:18 155:21,22 156:13,16 157:7 199:1 212:7,12,25 213:11 231:10,15 233:7 239:2 243:3 246:4 258:1 260:25 devices 22:23 26:7 34:9 35:21 36:12,15,25 37:12 38:16,18 45:17 47:11,18 73:12 76:5 77:5 101:7 103:1 113:10 144:11 148:17 151:17 156:1 212:19 213:19 230:11,15,22,24 231:4 232:15 241:3 245:18 246:6 250:5 258:20 259:4 dialogue 41:22 156:15 dictating 260:22 261:6 differ 50:6 difference 74:20 181:19 197:15 229:13 252:19 253:12 different 26:19 29:16 63:8 68:22 70:2 78:12 92:19 98:5 103:17,18 109:2 112:22 113:10 119:18 120:3 131:12,13	142:20 170:8 183:9 194:25 216:11 219:22 222:4 227:5,6,7 228:20 230:15 231:1,17 239:20 245:12 257:1 differently 211:6 227:21 difficult 37:24 81:9 101:10 164:19 170:10,20 216:19,25 digested 5:20 digital 39:4 57:20 75:9 113:9 diligently 232:10 diminishing 83:16 direct 42:12 119:5 directed 133:18 231:13 directing 211:25 direction 16:10 194:11 262:8 directly 44:2 100:22 139:10 156:11 171:1 199:18 226:13 256:24 director 209:22 210:5 directors 178:8 directs 59:11 disagreement 236:4 247:19 253:3 disassembler 48:11 discernible 58:14 disclosable 55:18 disclosables 58:4 disclose 31:21	55:14 80:2 81:8 86:15 89:9 90:5 105:5 153:15 154:18 155:10,23 156:20 175:4 180:8 187:5 197:18 204:18 disclosed 55:11 58:3 86:9 89:21,22 97:8 98:11 128:22 135:14 171:15 discloses 199:10 disclosing 36:4 38:6,11 78:15 79:7 140:10 154:2 163:15 disclosure 51:13,24 52:16 55:1 58:7,9 60:23 61:10,18 62:23 63:1,15 66:12 67:6 69:15 80:25 82:1 84:21 85:3,10 87:7 88:9,12 89:4,10,18,19 92:8,25 93:5,21,25 97:17 125:22 128:13,18,23 129:21 131:4 132:1 133:9 137:7,21 151:2,4,20 154:2,11,17 170:13 172:18,19,22 173:4 174:16,18 175:9 176:7,9,21,25 181:11,12,25 182:1,4 186:23 187:2 191:23 192:9 193:24 197:25 disclosures 125:14	126:20 disconnect 102:7 discounted 240:3 discourage 37:14 47:22 discouraged 259:20 discouraging 38:14 discover 38:7 89:16 126:24 175:23,25 176:1 discovered 11:5 36:11 54:16 72:11,17 73:13,14 75:18,20,22 91:13 96:7 97:3 151:6 191:9 discovery 56:20 95:25 132:18 189:6 191:15 discuss 22:17 30:21 35:15 42:7 50:4 54:14 55:4 157:4 discussed 22:2 33:21 70:6 73:4,18 89:20 199:20 239:10 245:7 246:3 discussing 12:12 50:3 92:23 161:2 discussion 11:17 50:8,9 119:3 124:11 145:21 203:7 205:12,19 248:8 discussions 145:21,25 199:16 dismantle 97:6 Disney 10:8 disposal 228:10
--	--	---	--

dispute 149:8 207:14 215:17,20 221:21 disputed 5:17 disputing 222:16 disseminate 68:8 127:1 130:7 disseminating 82:20 dissemination 52:7 132:17 dissuade 20:22 distilled 202:5 distinction 170:19 distinctions 183:13 distinguishing 142:4 255:8 DISTRICT 262:20 disturbing 190:9 192:13 DMCA 34:13 42:1,8,21,22 45:11 46:3 53:20 54:25 55:25 61:20 65:17 69:22 70:17,18 71:1 72:6,22 74:4,6 75:1,6 76:10,17 84:8,24 86:23 89:20 109:13 127:6 139:14 144:15,25 145:9 146:4 148:8,12,16 152:20 188:8 189:12 190:4,6 193:18 197:16 203:18,23 205:4 213:12 223:6 228:13 237:11 239:7	248:13,17,20 DMCA's 127:25 212:8 docket 95:4 doctoral 34:25 document 64:20 93:2 documentation 65:16,20 documented 54:8 63:22 dollars 176:3 dominant 79:16 done 15:24 33:17 34:7,16 36:18 42:21 72:24,25 75:5 78:10 101:4 111:18,22 119:16,22 128:14 159:8 166:16 180:1 198:3 219:14 255:25 256:1 Donna 210:2 247:23 248:4 door 38:12 59:18,20 60:10,15,20,21 64:14,15,23 66:18 67:14,21 68:5,7,11 110:8,12 113:7 156:6 225:25 doors 73:11 doubt 91:19 downsides 177:13 dozen 72:1 Dr 16:23 33:8 86:13 89:3 90:17 138:24 draft 29:22 202:2 260:7 drafted 247:25	252:14,19 dramatic 57:12 152:11 draw 184:13 196:23 drawn 182:21 211:6 drive 35:21 driven 199:9 200:5 driving 68:16 170:23 183:6 DRM 25:25 duly 262:5 Duo 198:12 duplicate 175:6 during 18:20 21:16 44:12 215:8 232:8 dynamic 33:16 <hr/> E <hr/> earlier 28:6 52:1 73:4 93:14 94:3,9 133:7 135:20 179:1 202:12 203:8 207:12 255:14 260:6,11 early 221:7 234:21 261:10 earned 125:7 easier 29:4 easily 58:14 225:22 232:18 easy 131:10,23 eBay 76:3 235:6 251:7,9 253:22 economic 97:19 238:22 economy 51:15 ECUs 133:24	134:2,6 Ed 21:16 edges 130:17 educated 52:15 educating 176:15 educational 73:23 74:17 EFF 20:16 effect 38:14 113:23 121:7 122:13 130:13 134:15,18 152:10 204:24 effectively 39:24 77:8 effects 21:23 23:2 116:9 119:9,11 127:13 160:11 effort 11:24 12:14,17 37:11 64:19 67:16 68:2 76:15 110:23 128:4 efforts 23:18 46:1 65:3 68:13 127:17 135:5 175:12 211:7 eight 68:21 160:4 either 66:19 72:22 130:23 147:2 213:1,6 241:15 259:8 elaborate 22:23 82:22 election 161:11 162:20 elections 161:6 electronic 18:3 19:21 72:14,16,20 161:4 electronically 74:22
---	--	---	---

electronic-control 133:23 element 59:12,23 60:14 61:2 105:15 111:7 196:8 elements 58:19 59:24 250:3 eliminates 214:23 elite 189:1 else 10:10,17 26:15 27:24 87:19 102:18 105:6 106:5,21 121:6,10 138:3 148:24 154:9 159:19 160:7,8,17,19 175:3 193:10 200:1 201:10 205:8 215:1 220:13 224:12 238:1 240:8 else's 110:12 148:24 e-mail 44:7 54:21 55:22 157:2 e-mails 217:22 embarked 18:17 75:7 embarrassment 151:23 embedded 200:18 embodied 202:6 Emergency 91:2 emphasize 163:15 249:1 emphasized 96:11 empirical 67:17 employed 262:10,14 employee 120:5 262:13	employees 156:8 employer 41:13 42:11,15 198:9 employing 179:24 enable 124:18 125:23 171:6 232:14 enables 31:25 enabling 145:15 166:14,15 enacted 69:24 112:22 127:6 144:25 212:4 215:6 245:5 enacting 84:12 86:23 127:5 enactment 72:6 126:13 211:24 encounter 218:15 encountered 11:22 encountering 179:8 encourage 94:2 95:25 119:23 134:21 135:8 152:21 181:10 191:19 207:18 encouraged 95:6 211:7 encourages 97:25 100:2 encryption 14:19 37:19 72:13 113:1,5 160:1 endangering 45:18 endorse 141:20 enemies 194:14 enforce 99:6 213:13 enforceable 99:2	178:16 enforcement 179:23 189:21 enforcer 100:7 enforcing 98:12 engage 41:12 51:7 53:8 56:6 76:14 77:13 87:22 92:3 125:24 135:5 152:21 158:15,21 186:23 187:5 188:8 239:16 engaged 63:1 69:9 107:12 117:17,18 178:18 189:20 213:1 253:11 engages 189:18 engaging 57:1 engine 133:25 134:2 engineer 76:6 77:5 engineering 12:22 14:20 173:20 185:16 engineers 41:12 enhancing 238:22 enormous 164:1 ensuing 232:8 ensure 23:17 25:6 131:18 153:13 232:17 ensured 45:8 ensuring 25:3 39:2 180:9 230:10 239:1 enter 43:23 entered 225:11 entering 71:25 enterprise 131:14 148:13	enterprises 131:20 entire 51:23 178:20 entirely 66:6 109:14 123:13 entities 52:25 96:24 entitled 109:11 entity 128:20 241:16 entrepreneurs 44:17 157:20 environment 31:20 32:7 112:20,21 environmental 134:11 envisioned 212:5 envisioning 169:21 170:11 EPA 145:23 equally 4:14 151:7 equation 200:9 equipment 77:12 212:14 equivalent 211:12 Eric 209:19 Erik 9:9 100:15 especially 5:13 6:7 essential 185:11,12 186:3,25 213:7 essentially 10:13 74:13,23 76:12 77:2 114:19 218:2 233:14,24 235:25 240:3 establish 214:9 established 213:25 esteemed 50:21 51:18
---	--	---	---

ETF 234:21	149:9 179:7	excuse 12:3 98:15	230:17,21
ethical 141:23	197:20 202:4	196:21	231:9,14,22
142:18,19 143:9	205:20 252:4	exempt 248:1	232:1,11,12,18
evaluate 20:11	examined 72:14	exempted 15:3	233:10 234:20
49:6	74:24 75:13	241:25	238:8 239:6
evaluating 131:15	examining 78:5	exemption	241:3,24
events 16:14 29:21	example 14:25	14:12,17 21:19	247:9,15,16,22,2
149:20	15:4 26:21 31:5	23:13 24:5,14	5 250:8,13
eventually 44:14	33:20 43:7 53:7	25:12,16,18,21,2	258:20
everybody	70:7 72:11	4 27:13,17,18	259:4,18,23
81:11,21 83:24	73:22,23 75:5	28:5,22 29:12,25	260:7,11,21
121:10 154:15	79:12,18 98:22	30:25 31:23 32:8	261:5
183:4 215:5	99:14 101:18	33:11,14 34:3	exemptions 14:25
everyday 22:21	102:7 103:8,19	35:9,16 38:22	16:8,25 18:7,12
167:12	104:15 105:23	39:1 45:11 50:23	22:2 23:16 28:17
everyone 4:3 7:3,4	112:4 139:10	56:2,6	35:14 37:19,22
30:1 68:7 89:16	146:22 151:10	57:3,16,18 66:9	42:8 93:8 113:12
105:6 130:16	153:5 154:13	71:16 88:8,17	127:12,21
177:21 192:9	155:2	93:11 94:2,19	137:12 177:15
205:22 207:15	158:10,13,17	95:2,14,20	202:23 210:19
210:12 261:11	159:13 161:1	100:19 106:9,20	211:17 232:7
everyone's 153:5	162:11 164:21	107:19 108:19	239:12,13
everything 185:12	166:1 167:19	110:21 111:4	245:22 247:13
196:14	174:14 183:23	114:3 115:14	257:4 261:12
227:11,14	193:19 201:21	117:22	exercise 47:21
evidence 7:7,9	203:20 257:14	119:8,15,21	exhibit 4:4
24:7 87:21	examples 45:6	124:18 125:2	7:11,13,14
134:17 152:9	71:4 72:21	127:20 129:9	53:23,24 54:2
192:11	103:18 104:10	130:8 132:24	73:4 123:1,17,21
evokes 28:24	182:8	135:11	151:13 156:1,2,4
evolve 259:9,24	ex-ante 16:20 61:4	136:17,23,25	173:14 195:7,21
evolved 27:15	except 47:21 91:11	137:14,15	exhibits 43:23
219:21	184:9	142:17,23	208:6
evolving 22:8	exception 18:6	143:13,19,25	exist 58:3 122:15
26:3,5 199:16	109:17 260:24	146:15 147:11	174:24 175:3
ex 114:21	exceptions	152:15	190:3 191:1
exacerbate 128:24	127:6,10 128:1	170:12,21 177:3	203:16,23
exact 123:1 132:7	excerpt 49:25	180:15	existed 60:20,21
149:7	excess 56:22	190:14,15 192:3	existence 182:5,17
exactly 11:13,14	exchange 55:23	199:24 201:20	existing 24:23
28:9 55:9	excited 124:3	202:14 203:5	51:13 63:3
107:5,16 111:10	exclude 143:19	204:4 209:12	127:21 137:12
130:9 146:15	226:9 229:5	211:2,3,4,6,10,2	181:6 215:25
	250:5	0 212:3 214:2	232:7
	excludes 247:16	215:9,20	exists 23:24 57:9
		216:1,10	59:10 67:4
		224:15,17,24	
		227:24 228:23	
		229:5,15	

<p>222:17</p> <p>ex-NSA 192:19</p> <p>expand 254:12</p> <p>expanding 212:1</p> <p>expanse 212:5</p> <p>expansion 70:20</p> <p>expecting 11:14</p> <p>expense 151:22</p> <p>expenses 38:20</p> <p>expensive 12:17 74:14,15</p> <p>experience 19:1 45:5 52:21 54:22 218:7</p> <p>experiences 93:23</p> <p>experimentation 140:6</p> <p>expert 36:21 96:10,11</p> <p>experts 122:2</p> <p>expires 262:22</p> <p>explain 13:16 41:10 49:3 120:3 155:19 170:1 185:2,3 197:19 212:16 216:15 232:22 241:25 250:12</p> <p>explained 153:7,9</p> <p>explaining 7:19 47:6 54:22 55:23 166:2 195:16,19 196:11</p> <p>explanation 118:21 260:15</p> <p>explicitly 247:8 250:13 256:14</p> <p>exploit 10:10 107:3 129:1 166:13 167:4 168:2 172:21 175:17</p>	<p>182:6,13,19 183:10 185:13</p> <p>exploitable 96:16</p> <p>exploitation 125:24 145:1 185:7,9,16</p> <p>exploited 10:16 91:7 97:3 125:4 161:10 165:4,5 166:3 180:16 232:18 247:17</p> <p>exploiting 24:23 83:23 177:14 183:20</p> <p>exploits 92:10 175:20 180:24 181:1</p> <p>explore 30:13</p> <p>exploring 88:19 118:7,11,19</p> <p>export 126:23 159:21,22,23 160:10,13,22</p> <p>expose 96:12 151:19</p> <p>exposed 96:20 141:2</p> <p>exposes 191:24</p> <p>exposing 96:8</p> <p>ex-post 16:20</p> <p>exposure 11:2</p> <p>express 231:23</p> <p>expressed 78:6 232:5</p> <p>expresses 56:19</p> <p>expressly 171:8 202:20 245:17 246:20 247:16</p> <p>extend 210:21 261:5</p> <p>extended 21:10 224:4</p>	<p>extends 257:25</p> <p>extensions 136:4</p> <p>extensive 178:4</p> <p>extensively 92:23</p> <p>extent 30:23 31:1 86:24 87:15 116:6 137:10 143:4 145:11 177:5 202:21 256:12</p> <p>external 53:13</p> <p>extract 75:25 76:5,8</p> <p>extracting 78:2</p> <p>extraction 148:19</p> <p>extraordinarily 12:23 136:10 177:2</p> <p>extreme 139:7</p> <p>extremely 77:3 125:11</p> <p>eye 215:7</p> <p>eyes 44:12</p> <hr/> <p style="text-align: center;">F</p> <hr/> <p>face 10:24 23:9 158:17</p> <p>Facebook 52:25 200:20</p> <p>faced 96:2</p> <p>faces 187:24</p> <p>facilitate 15:11 16:5 27:1 31:6 128:11 170:15</p> <p>facilitating 31:12</p> <p>fact 12:1 15:5 52:24 53:2 58:10,15 60:19 85:4 87:18 90:2 101:25 117:16 119:20 125:2,18 134:19 136:3 140:20 146:22</p>	<p>158:19 179:6 181:2 247:14</p> <p>factor 33:11 86:9 229:2</p> <p>factors 87:13 103:5 171:13</p> <p>factory 196:12</p> <p>facts 31:15 128:15 149:7 150:23 192:16</p> <p>faculty 46:21</p> <p>failed 55:15 99:22</p> <p>failing 98:23 99:13,16</p> <p>fails 15:1</p> <p>failure 61:14</p> <p>failures 75:20,23,25 77:6 97:25</p> <p>fair 84:25 104:1 105:17 137:5 243:8</p> <p>fairly 73:20,22 83:21 137:3,4 161:12</p> <p>fair-use 245:14</p> <p>faith 16:2 21:25 24:13 29:20 37:18 38:6 78:16 104:11 109:4,8 177:8 204:23</p> <p>faithful 105:24</p> <p>fall 16:24 29:12 88:16 104:11 105:10 106:8 108:19 203:24 225:23 249:10</p> <p>falling 127:2</p> <p>falls 162:5</p> <p>familiar 40:2 82:8 194:3 207:23 218:12 219:12 240:11</p>
--	---	--	---

familiarity 260:17	figures 192:23	92:15,20,22,23	45:9 47:11 51:13
family 219:15	figuring 244:5	96:5,17 100:25	72:12,15 73:14
225:10	filed 35:7 93:7	101:3 128:19	79:7,12 90:20
236:13,14,17	211:1,3 248:20	130:5,11 147:5	91:7 147:7
famous 195:7	filing 135:21,22	148:2 150:1,16	158:22 175:22
Fandango 99:16	136:13 153:24	153:10,12 161:8	199:10 203:24
fashion 258:14	154:1 202:5,17	175:25 181:18	flexibility 214:23
favor 159:7 225:5	247:14	196:10 197:7	222:24
favorite 153:5	filings 92:21 93:3	211:16 214:16	flight 147:1
FBI 145:8	final 44:7 193:8	240:24 245:7	flow 70:5
FDA 145:23	finally 41:22	248:9 255:7	flows 70:14
fear 41:25 46:3	93:10 156:17	firsthand 253:15	fly 147:1 255:12
74:5 204:22	178:18 189:15	fit 208:11 249:17	flyer 150:21
fears 75:2 143:4	247:11	252:6,8 259:4	focus 27:23 71:20
features 22:24	financial 54:10	five 24:7 124:5	95:7 207:18
40:25 97:15	125:25 130:23	174:7	212:17
134:4	financially 262:14	five-minute 124:5	focused 33:14
federal 75:10,17	findable 67:15	fix 21:24 74:13	focuses 5:24
98:22 99:2 100:7	finder 60:19	83:11,24 90:24	focusing 146:9
193:12	finding 10:19 97:2	91:25 92:6	folks 14:21
fee 221:7	192:25	128:20 131:12	15:2,25 27:16
234:15,22	fine 90:16 237:21	135:13 152:23	32:21,23 118:2
feel 93:13 143:13	242:10 258:25	154:20,21	144:9 145:22
152:13,20	finer 16:18	162:10,20	follow-up 55:22
188:25 221:21	finish 19:12 254:2	168:16 179:3,10	footnote 92:22
feelings 205:15	finished 193:8	195:25 196:5,19	forbid 15:14
feels 199:19	219:1	fixed 46:12 63:10	forced 38:19 63:5
fees 234:11	firewall 174:2	96:7 131:25	foregoing 262:3,5
fell 240:17	firewalls 49:1	140:11 151:18	foreign 159:23
fellow 4:21	90:22 148:14	153:14,16	foremost 192:18
felt 19:25 42:15	firm 38:9 42:17	fixes 91:7	forgive 40:2
57:20 94:8	54:1	fixing 45:9 142:8	forgot 56:13
162:14	firmware 76:1,5,8	flaw 35:25 36:13	form 35:8
Felten 21:16	101:8	41:5 47:5 54:17	formal 189:23
fewer 230:6	first 11:2,10	62:15 73:13	204:13
fielded 72:8,16	21:13,15 23:20	74:19 78:20	format 5:21
fight 58:9 157:23	48:22 49:1 53:15	91:10 120:12,16	former 21:19
figure 49:18 56:21	61:7,8 67:2,10	121:1,2,8 141:3	198:9
64:24 68:3 86:15	71:14 73:2	189:14 191:1	forms 176:6
104:14 107:4	75:9,16	194:24 195:2	formulation
185:17 236:9	85:11,20,24	flawed 40:25 42:4	233:2,3 252:25
	86:23,25 87:8,15	47:18	
	88:2 91:1,14	flaws 10:15	
		21:22,25 23:23	
		26:13 27:10	
		31:18 38:2,6,11	

257:13,21 forth 15:12 66:22 70:14 171:15 211:18 fortunate 19:20 20:15,17 forum 135:1 forward 4:13 19:23 25:14 39:6 71:9 100:11 142:22 201:3 203:10 211:13 231:8 242:17 243:11 261:18 Foundation 18:3 19:22 37:9 frame 125:5 framing 202:7 203:15 frankly 47:21 226:18 fraud 120:8 125:25 203:20 243:3,4 250:6 freaking 197:12 free 16:6 85:7 218:3 221:21 227:3 freedom 159:18 160:20 frequent 150:21 frequently 188:25 189:6 207:21 friendly 44:9 frivolous 51:11,19 56:7,8 71:7 74:6 75:1 93:10 116:9 front 16:1 29:2 39:8 59:17,20 60:9,15,20,21 64:14,15,22 66:17 67:14,21 68:4,7,11 99:13 136:13 156:6	197:10 Frontier 18:3 19:21 fruition 215:5 FTC 99:15,19,24 178:17 179:11,19,22 189:15,16,17 190:3 FTC's 190:5 fulfilled 243:21 fulfilling 223:19 242:24,25 full 23:5 43:11 56:3 93:2 207:19 213:14 217:24 245:13 254:15 fully 117:23 158:11 211:18 216:16 255:11 function 164:24 189:19 213:8 259:5 functionally 211:11 functioning 212:21 functions 133:24 134:1,2 fundamental 72:12,18 75:19 159:18 160:4,5,9 213:16 fundamentally 80:16 212:6 funded 33:23 37:8 91:3 funders 113:20 funding 72:4 159:15 funny 140:15 Furthermore 38:1 future 172:16	245:22 <hr/> G <hr/> gain 10:11 game 52:13 games 22:19 25:17,19,24 26:1,14,18,21 27:7,15,18,23 gap 233:18 gathered 41:8 Gazelle 251:10 geared 202:20 general 4:8,23,25 5:1 9:15,17 10:14 54:21,22 55:21 56:14,15,17 57:6 113:22 122:7 187:10 206:16,23,25 207:1 generally 47:3 62:12 103:22 163:7 173:1 184:14 185:24 187:22 generated 157:19 genuine 200:24 George 209:14 Georgetown 209:10 germane 204:21 gets 15:5 66:1 144:4 153:17 155:6 174:6 176:24 188:3 251:12 getting 17:3 56:20 72:4 76:25 84:11 116:22 140:10,25 144:24 155:16 156:22 164:10	175:13 212:7 213:3 226:4 258:16 given 152:11 172:24 262:9 gives 61:8 67:15 159:15 160:19 185:13 205:8 237:2,3 giving 46:17 52:5 61:4 182:12 184:21 236:20 GM 133:22 178:2,4,9 182:25 183:3,25 goal 5:11 6:5 10:14 42:24 70:9 113:2,11 124:20 129:15 goals 143:15 God 15:14 147:1 gone 44:19 55:9 66:22 good-faith 10:25 20:18 21:20 23:17 25:13 35:11 36:7 39:1 63:21 64:19 67:16 68:2,13 108:21 110:23 111:21 124:19 128:4,7 129:16 188:16 235:25 Goodlatte 246:20 goods 22:21 Google 53:1 81:17 82:12 83:9 88:11 93:6,8 155:4 197:8 200:21 Googled 196:8,10 Google's 93:4 gosh 166:23 government 37:8 72:20 75:10
---	---	--	--

126:12 188:23 192:22,24 209:22 government- proposed 72:12 governments 161:17 162:3 governs 85:16 grad 13:3 19:25 graduate 11:3 18:14 20:14 75:7 grant 21:19 25:11,12 29:25 35:13 38:22 56:5 66:8 119:15,21 142:22 159:13,15 190:14 215:21 granted 16:8 25:17,21,24 27:8 56:3 125:2 135:11 136:5 grant-funded 160:18 granting 95:20 117:21,22 119:8 202:24 204:4 230:16 granularity 197:24 great 11:22 33:25 34:15 40:17 49:22 94:15 109:18 157:11 177:6,10 180:23 209:13 greater 239:1 Green 7:25 8:1 9:22,24,25 12:7,9,11 13:11,13,19 15:15 16:13,16,23 17:14,22,25 18:19,25	19:4,7,9,13,15,1 7 22:12 23:5,19 24:17 29:1 32:12 33:1,8,13 34:6 35:6,8 36:1,20,23 37:4,7 38:8 80:21,22 81:14 82:23 83:2 86:13 124:21 138:24 139:1 141:15,23 144:6 154:8,10 166:5 204:17 Green's 32:18 153:24 grey 160:15 162:5 180:12,24 188:19 204:19 group 166:15 grown 53:10 guarantee 18:6,13 guaranteed 215:12 guarding 127:1 guess 16:18 28:20 32:3 63:5,20 66:22 68:16 112:10,11 144:2 177:10 191:22 206:2 guessing 69:7 205:17 guidance 30:18 31:2,15,24 112:1 guide 245:5 guy 146:25 217:20 guys 8:11 24:17,22 91:7,15 96:12 124:23 125:4 148:14 166:17 176:8,9 <hr/> H <hr/> hack 52:7 126:23 146:25 147:5,24	148:1,8 149:3 164:11 165:19 168:19 169:1 184:23 197:6 198:24 hacked 41:15 140:15,17 hacker 91:19 192:19 hackers 48:23 96:19 197:6,7 hacker's 91:18 Hackers 49:2,24 hacking 52:11 138:6 148:5 194:3 Halderman 21:14,15,21 Halderman's 24:1,8 half 96:21 146:9 156:19 176:2 hall 206:4 hallmarks 53:13 hand 68:10 141:2,3 218:9 221:15 handful 103:17 handing 221:14,22 handle 66:24 179:6 handles 196:7 handling 53:11 58:22 60:3 hands 127:2 188:5 240:18 handset 216:2 243:24 handsets 3:4 208:14 210:20 211:4,11 216:5	230:11 231:4 happen 11:14 81:21 145:22 184:23 189:7 192:6 227:15 happened 11:21,22 17:2 34:15 75:3 141:25 149:10 153:7 192:11 214:1 236:10 happens 65:15 67:24 84:21 103:22 177:11 217:14 happy 4:6 46:7 86:2 93:2 129:18 199:18 211:14 261:9 hard 7:16 13:5 17:1 27:9,13 29:1 62:1 66:15 78:19 111:9 120:16 169:10,21 177:3 194:19 195:5 202:2 204:17 226:3 227:16 255:12 hardest 194:18 hard-pressed 146:22 harm 22:6 25:8 45:7 50:12 79:6,9 80:12 97:21 214:2 230:17 247:18 248:12 harmful 184:24 harms 213:23 harm's 44:25 45:14,15 Harris 209:19,20 238:5,6 239:23 240:5,24 242:1,9,13,21
---	---	---	---

<p>243:5,9,14 Harris's 247:11 Harry 9:14 hat 101:22 135:3 hate 114:18 115:1 haven't 256:21 having 57:3 64:8 66:13 67:10 74:6 106:3 119:2 127:13 139:18 145:25 157:2 159:21 169:19,22 170:10 196:15 215:12 236:7 head 225:16 heads 66:5 headsets 238:9 hear 6:14 22:11 27:16 40:6,7 121:5,6 136:1 140:14 195:2 222:12 229:20 heard 23:4 31:8 49:17 52:1 119:10 129:21 156:24 207:11 hearing 4:11 5:11 21:11 43:23 52:19 53:24 54:2 55:8 73:5 84:3 86:12 87:10 88:13 147:2 171:10 255:7 hearings 1:6 4:11,12,14 33:22 207:12 heart 170:17 213:15 Heartbleed 36:13 82:7,25 83:6 107:2 heavily 95:7,9 held 43:15 124:13</p>	<p>185:24 205:15 206:9 Hello 210:13 help 24:21 46:1 51:18 53:3 62:6,8 97:18 99:12,25 107:7 129:16,17 151:5 156:5,8,9,12,14 226:8 helped 51:5 helpful 5:16 30:13 61:3 86:4 116:12,16,17 237:23 242:2 253:7,25 helping 45:13,14 232:17 helps 7:9 245:5 hence 201:1 Heninger 36:2 62:23 63:2 Heninger's 63:12 hereby 262:3 263:2 here's 49:3 86:6 91:12,13 182:9,11 183:10 192:25 216:21 hereto 262:14 he's 55:25 117:2 168:11 192:19 193:5 208:22,23 210:5,7 227:5 Hey 26:10 Hi 4:20 9:6,9,12 206:20 209:19 210:2 243:17 248:4 hidden 180:11 219:16 hide 13:7 high 48:6 83:9,21</p>	<p>140:11 168:7 201:17 highest 178:8 high-five 192:23 high-level 164:9 172:18,19 174:16 207:25 highlighting 23:8 hijacking 146:18 hinge 109:13 hire 101:21 hired 103:10 hiring 56:25 history 35:17 48:6 91:13 110:5 112:13,24 117:6 246:8 hit 249:21 Hogan 9:17 hold 234:3 holding 39:17 home 43:13 45:20 207:13 231:19 232:22 home's 43:8 homework 49:9 homicide 150:1 Honda 196:8 hone 5:16 honest 254:21 honestly 42:25 honorable 48:17 hook 227:6,10 hope 14:15 16:9 119:1 142:11 149:16 190:17 255:10 259:5 hopefully 36:2 138:3 150:5 201:23</p>	<p>hoping 222:23 Hopkins 8:2 10:1 horrified 150:22 hostile 59:14 77:15 hotline 190:1,2 house 73:15 112:25 260:19 HSBC 112:4 HSBC's 106:14 huge 34:2 138:11 hugely 174:18 175:7 human-generated 63:7 hundred 49:20 230:5 hundreds 121:3,10 150:4 hurt 92:9 husband 237:3 hypothetical 17:25 227:8 hypothetically 17:15 183:24 hypotheticals 226:21 236:20 <hr/>I <hr/>ICS 63:13 I'd 30:23 34:20 35:12 52:17 72:21 73:2 82:7 93:1 138:8 143:22 144:3 152:7 154:10,16 254:8 255:14 idea 143:21 171:3 233:10 252:10 255:11 257:14 ideally 97:3 identically 211:10</p>
--	---	--	---

identification 54:3 123:22	50:24,25 55:7 59:22 65:4 69:6 71:18,22 76:20 78:12 80:18 86:12 87:2,9 88:13 89:4 100:15 101:19 102:6 103:7,9,11,15 104:14 105:13 106:13,22 108:2,3,13,14 109:7,9 111:3 114:7 115:22 117:12 120:5 124:16 131:9 133:2 139:15 141:8,15 143:17 146:22 147:13,22 148:8 151:10 155:14 160:24 164:13 165:8 166:11 167:6,14,17 169:22 170:10 171:3 172:13,14 174:25 175:1 177:18,19 182:20 183:6,17,24 194:3,15 196:23 198:5 204:6 205:11,17,19 206:15,17,24 207:5 208:16,17,18 209:9,11,14,21 210:2 214:4 216:12 218:6,12,20,21 219:5 220:8,10 222:17,18 225:17,19 226:2 227:2,3 236:20 238:6 240:19 245:1 248:4 250:11 251:20 259:11,12,17	251:6 immediate 9:16 61:8 225:10 236:17 immediately 80:15 162:15 impact 51:14 73:24 133:19,21 impacted 45:10 63:17 impair 246:22 impediments 121:25 122:22 imperative 38:21 implanted 199:1 implement 11:8 98:24 99:17 182:7 implementation 71:23 75:23,24 77:6 189:22 implemented 74:21 implementing 126:22 158:6 172:4 implicated 201:20 205:3 implications 92:24 164:2 172:1 import 47:14 importance 36:7 49:21 125:8 163:15 important 30:20 32:1,15,17,25 33:16 37:16 47:14 59:2,12 60:14 79:8 85:8 98:1 126:19 127:22,23 134:4 151:8 164:18 165:1 166:7 167:9 174:18	175:7 187:25 197:23 205:16 212:19 229:2 238:21 245:4 247:13 253:17 importantly 113:19 128:13 129:15 245:25 impose 37:23 imposed 259:23 imposing 216:18 impossible 244:1 impractical 244:1 improvement 58:13 improving 100:9 199:11 200:16 inaccurate 173:16 inadvertently 129:17 inappropriate 248:13 incentive 97:19 134:21 incentives 126:10,16 180:10 217:19 incentivize 130:22 incidence 57:15 incident 56:16 145:4 149:7 incidental 213:5 include 22:22 116:10 133:22 144:5,6 165:23 185:6 212:2 250:5 260:8 included 26:18 37:18 70:6 89:17 121:24 127:8 includes 122:8 230:4
identified 131:17 137:23 198:10			
identify 63:17 102:15 103:5 125:25			
identifying 53:7 55:24 79:11			
idly 108:23			
ignored 77:13			
ill 96:14 127:9			
I'll 4:17 5:10,21 32:11,14 35:14 43:14 55:12 56:13 114:11 121:19 133:17 153:23 180:21 181:16 203:7 210:25 214:8 220:13 225:17 240:14 243:9			
illegal 48:19 144:12 145:15,17 225:6,7 239:13 247:17 248:1			
illicit 241:10			
illuminating 205:12			
illustrated 22:13			
illustrative 73:23			
I'm 4:3,6,8,13,20,24 5:5 7:17 8:2,10,24,25 9:1,3,6,14,25 10:4,19,22 13:9,12,21 14:21 17:15 20:3,8,15 21:3 27:4,10,11 33:21 34:25 35:3,14 36:16,25 39:16 46:19 49:20,22	imagine 103:8,15		

including 14:17 24:16 36:13 43:11 44:19 82:12 97:17 121:23 128:12 135:1 159:25 160:12 255:21,22 incorporate 97:11 incorrect 136:20 incorrectly 205:9 increase 175:14 210:22 increases 20:21 increasing 10:22 21:22 176:5 238:24 increasingly 22:20 incredibly 116:12 189:18 incur 38:19 indeed 36:1 142:7 158:5 160:15 indemnified 161:25 indemnify 162:4 independent 36:7,11 37:6,14 47:1,16 56:24 58:24 60:5 67:11 99:12,20 124:24 125:9 130:20 134:24 indicated 145:4 178:6,15 179:21 195:1 indicates 95:14 154:1 indifference 45:4 indispensable 125:7 individual 83:12 149:15 174:20	177:7 193:18 199:10 222:20 225:8 238:18 individuals 33:23 34:8 82:4 199:17 201:10 individual's 231:19 industrial 74:18 238:14 Industries 209:21 industry 10:5 62:5 74:9 133:20 134:16,21 135:1,3 152:9 158:24 159:2,3 178:10,11,20 196:6 inequitable 222:14 inevitable 81:25 informal 78:24 information 10:25 15:6,9 18:16,19 26:22,25 31:10 42:8 44:12 52:24 55:5 63:4 70:5,14 81:4,19,22 82:20 83:10,21 96:9,20 97:14 98:15,20 99:1,4 126:20 128:8,14,19 130:24 142:23 153:15 165:15 166:7 167:9 169:16 172:25 173:17 178:14,21 180:5 182:15 184:9,22 185:13 193:24,25 200:16 231:6 information-sharing 126:9 informed 97:18	99:21 163:19 168:22 informing 57:7 infrastructure 51:16 54:11 114:14,17,20 126:1 infringement 15:12 16:6 17:9 27:2 31:6,7,12 128:11 145:2 146:21,23 147:4 202:15 212:13 infringing 89:13 147:14 initial 85:4 153:24 243:18 245:15 initiatives 126:19 innocent 150:5 251:8 innovation 209:25 210:4,6,23 245:2 248:5 259:20 innovators 157:20 inquire 150:6 inquiry 245:21 insecurities 38:3 installed 110:11 installment 233:7 instance 42:9 76:22 112:7 179:11 197:17 237:4 instances 47:12 55:24 56:17 65:19 121:11 205:2 instead 11:21 12:11 240:6 246:24 Institute 9:8 209:9,20 institutions	113:19 134:25 instructions 165:18 167:3 169:1 172:20 183:11 insufficient 101:3 170:7 214:11 insufficiently 55:11 intake 189:23 200:6 integrated 137:13 integrity 70:12 200:17 intellectual 51:6,7,8 intelligence 193:3 intended 12:24 37:17 127:14 148:17,21 240:2 246:21 247:1 intending 202:14 intent 13:6 28:19 84:12 87:17 106:11 111:25 127:24 129:11 137:11 143:15 260:14 intentions 127:3 interacting 54:23 interacts 159:11 intercept 167:20 168:19 interest 7:20 38:1 52:5 78:6 79:5 124:23 130:20 192:21 203:6 209:3 230:9 interested 5:8 6:7 52:17 122:4 143:23 262:15 263:5 interesting 47:8
--	---	--	--

73:22 113:8 193:2 194:1 interests 52:20 124:25 153:20 interference 8:4 interim 260:23 intermediary 193:15 intermingled 22:20 internal 53:7 58:21 60:2,7,11 61:5,14 64:9 65:10,20 66:15 67:7 69:9 200:7 internally 66:25 International 209:22 Internet 22:22,25 43:3 49:1 82:4 83:13 92:4 93:6 108:6 147:25 157:19 Internet- connected 39:14 72:9 Internet-enabled 101:7 interpretation 116:24 117:24 118:1 119:7 139:16 interpretations 118:4 interpreted 223:6 246:12 interpreting 118:25 interpretive 58:15 interrupt 6:2 13:10 207:21 214:5 intertwines	203:17 intervening 24:7 intervention 63:13 interviews 192:20 in-the-moment 61:8 introduce 4:18 7:18,19 206:18 introduced 102:19 210:24 260:9 introduction 9:15 introductory 238:10 inundated 45:16 invest 97:20 investigating 31:18 inviting 34:22 94:17 invoke 202:14 involve 11:17,18 12:20 133:7 147:8 183:20 involved 36:23 37:1 50:1 84:24 194:3 206:7 209:25 224:21 involves 20:9 26:11,12 185:9 involving 148:7 IOActive 38:10 54:6 73:3,14 74:24 IOActive's 56:14 IP 209:25 210:3,6 245:1 248:5 iPhone 120:17 218:23,24,25 226:22,23,24 227:1,4,12 ironclad 119:13 irresponsibly	120:10 isn't 34:5 52:4 102:11 103:4 129:3 165:18 169:4 183:8 248:16 ISO 66:13 68:20 84:18 88:10 187:16 198:21 199:15,21,23,25 200:4,8,10 201:7,14 202:6 ISO-compliant 158:18 ISP 102:22 ISRI 209:20 210:1 229:15 235:2 238:13 244:3 245:2,13 248:6 249:18 252:25 256:1,9 258:18,19 ISRI's 238:7 239:15 243:25 247:2 249:1 251:9 issue 4:4 6:18 14:1,4,7 17:21 21:8 25:20,23 36:18 50:1,23 51:24 66:12 81:2 84:4 89:4 94:9,17 100:11 105:9 107:18 109:20 120:11 121:1 122:18 131:2 137:7,22,23 138:10 146:20 150:25 154:4,16,19 157:4 174:24 176:7 179:1,12,14 180:6,22 197:4 201:15 205:16,17,18	213:10 222:8 227:21 232:22 241:1 255:3 258:11 260:16 issues 5:25 6:6 13:22 14:3 21:5 30:21 41:10,23 44:2,6,7,11,14 51:1 66:13 70:13 71:1 85:20,24 92:19 94:21,22 95:8,9,16 126:8 137:22 139:2 140:7 150:13 155:23 156:9,17,22,25 159:6 162:7 199:19,22 207:13,18 229:17 240:21 243:12 248:18 255:1 items 55:18 156:3 iteration 199:22 it's 5:16 7:15 10:15 13:5,6 15:4 17:1,5 21:8,9,12,14 26:13,14,15 27:9 28:25 29:14 30:13 32:15 35:23 39:20,22 40:3,15 47:8,19,23 48:1,3 49:11 50:7 53:12 56:8 61:2,25 62:17 64:7 65:13 66:14 69:1 72:24 76:13 77:19 80:5,13 81:24 84:7,11 85:8 89:22 92:3 95:5,24 102:3,14,24 103:3 104:17,25 107:7 113:8 117:8 118:3 119:18,20
---	--	---	---

120:12,25 122:16 123:16 125:18 129:25 131:18 138:15 140:15 142:17 143:8,17 146:14 148:16,21,24 151:11,18,22 154:12 159:19,20 169:12 170:24 171:7 174:2,7,19,20,22 176:7 177:2 178:6 180:12 183:6,14,18 184:11 185:19 186:25 187:1 192:12,13 193:19 194:19,21,22 195:14,17,24 198:25 201:25 202:2,18,23,25 204:17,18 205:14,16 207:10 210:11 215:4 216:25 217:2,10 218:14 219:16,24 220:17,18,19 221:21 224:25 226:2 227:6,25 228:4 234:10,21 235:4,6,25 236:16,17 242:23 250:4 251:13,24 255:12,20,22 257:9,13,19 261:2 I've 51:5 62:2,6 72:24,25 75:5 81:20 94:22 101:14 102:2 103:9 173:18 217:16 226:22 227:2 229:12 239:19	<hr/> <div style="text-align: center;">J</div> <hr/> Jacqueline 2:2 4:8 206:15 JANE 263:2,18 January 164:22 job 142:21 158:12 John 2:9 5:3 207:3 Johns 8:2 10:1 join 6:6 36:2 joined 4:16 46:21 211:5 joining 35:3 joins 36:10 Jones 54:5,23,24 55:15 57:19 journalistic 172:11 judge 60:18 64:18 judging 64:10 judgment 28:24 29:7 64:13 84:5 85:2 125:15 142:12 205:7 judgments 84:13,14 85:18 Judiciary 232:5 judicious 128:18 judiciously 128:14 jumping 216:12 June 263:18 <hr/> <div style="text-align: center;">K</div> <hr/> keen 230:9 key 5:25 73:10,15,16 154:4 231:20 keyed 73:25 kick 32:11 kicking 210:15 Kickstarter	157:21 killing 150:4 kinds 30:5 74:19 196:7 197:21 219:20 222:24,25 kings 114:21 knew 19:2 91:1 163:6 194:7 knowledge 38:2 41:17 47:9 188:2 253:15 known 74:11 98:7 165:12 166:16 189:4,10 <hr/> <div style="text-align: center;">L</div> <hr/> L.A 6:18 142:20 150:12 Laboratories 72:1 laborious 188:5 Labs 46:22,23 lack 45:4 149:11 150:9 laid 226:21 language 26:18 28:23 29:14,22 30:6,13 70:7 105:1 110:24 242:9,15,16,18,2 0 243:25 246:14,19,24 249:1,4,11 250:4 252:19 260:8,12 large 5:8 39:4 45:12 76:15 80:7 99:11 149:13 157:22 158:8,12 largely 65:8 larger 106:25 148:4 largest 11:7 last 4:12 22:5,9	27:12 36:1,9 39:13 42:19 80:24 90:21 96:18 99:14 144:16 160:3 177:22 189:17 202:5 203:14 204:12 212:4 219:21 later 43:24 48:22 49:14 61:18 67:7 93:18 155:8 latitude 177:13 217:14 laughter 140:15 launch 208:15 Laura 9:6 179:20 law 8:15,18 9:2 13:6,15,20 17:18 18:7 24:18 25:9 35:4,5 37:25 52:18 54:1 57:9 58:16 69:5 84:10,13 86:18 98:21 122:15 128:12 133:8 139:11 144:17 146:3,13,16 150:9,11 159:21 160:3 162:1 171:17 191:12 202:2,25 203:4 207:19 209:11,17,24 210:3 213:13,17 215:7 233:3 238:11 239:9 245:1 246:16 256:5 lawful 143:8 217:5 246:5 255:18 256:15 lawfully 128:3 238:17 242:6 244:5 249:6 laws 99:3 121:22 139:9 144:7,13
---	--	--	--

145:16,18 146:1,9,14,18 150:1 152:17 159:21 160:13,22 204:6 lawsuit 13:4 20:1 43:1 lawsuits 248:20 lawyer 20:11 139:16 lawyerly 17:11 lawyers 20:19 lay 15:19 Lazarus 209:16 229:21,22 233:1 234:8,13,19 235:13,16,19 236:3,15,22 237:15,22 238:1,2,4 244:9 249:24 250:14,17,19 251:11,14,17,20 252:4,6,18 253:2,10 256:9 257:12,19 258:24,25 lead 9:22 50:8,11 73:19 75:23 140:6 199:17 leader 178:4 leadership 45:2 leading 230:2 leak 81:3,19 82:6,9 83:22 leaks 83:21 leaning 203:10 learn 185:4 learned 48:7 91:20 least 30:18 42:15 47:24 52:5 66:5 88:16 95:13,22,23 99:15 104:25	112:1 136:15 141:10 143:25 167:1 215:9,18 217:9 219:3 222:14 226:9 leave 121:19 141:15 256:16 leaving 185:16 186:25 234:15,16 led 117:21 196:14 205:5 211:22 legal 10:22 12:18 18:23 20:20 38:20 41:14,20 42:10 46:3 50:25 53:17 54:25 57:1 67:12 76:15,22 77:19 93:17 121:25 122:14,18 141:16 145:13 157:22,23 159:10 170:11,19 228:9,25 248:10 249:9 legalized 253:5 legally 212:15 239:5 241:20 legislation 73:1 126:9 211:25 215:6 legislative 94:23 110:5 112:13,24 117:6 246:8 legitimate 104:10 113:4,13 181:20 213:14 227:23 228:4 241:13 246:22 legitimately 148:18 legs 124:6 lend 70:19	length 237:14 lengthy 24:10 Lesley 197:10 less 17:25 29:17 30:7 57:19 58:11 74:14 80:13 93:20 141:6 259:22 lets 160:17 let's 6:14 60:20 79:18 81:15 108:13 138:21 167:19 168:15 177:16 180:20 206:1 225:14 229:1 236:12 letter 18:18 39:25 53:25 54:5,21 55:2 letting 221:23 level 26:20 85:12 159:1 168:7 170:8,14 levers 12:16 levied 61:16 liability 38:19 126:17 216:24 228:13 233:21 234:2,3 239:7 liberty 57:20 librarian 15:24 25:12 247:4 261:4 libraries 79:13 Library 1:4,8 license 120:23 licensed 101:9 117:14 121:12 lie 256:11 life 23:22 62:18 213:19 life-saving 35:21	life-threatening 182:25 light 232:3 Lightsey 9:14 133:14,15 152:6,7 153:2 177:24,25 Lightsey's 177:20 likelihood 119:8 likely 47:20 57:19 119:11 230:17 limit 141:9 231:14 258:9 limitation 30:23 31:5 32:20 33:4 101:3 137:4 202:17,22 215:24 limitations 27:3,21,25 30:5 31:3 32:2 85:12 87:23 143:12 limited 25:17 33:12 80:9 135:15,23 136:18 161:12 189:20 213:3 224:24 231:23 254:22,24 255:22 limiting 126:17 226:16 limits 236:21 line 38:11 54:18 59:8 76:11 131:19 144:16 149:22 150:1 182:20 183:11 184:14 206:18 line-by 183:10 line-by-line 168:25 line-drawing 142:24
--	--	--	--

<p>lines 78:11 161:2</p> <p>Linux 101:20</p> <p>list 28:16 36:10 58:3</p> <p>listening 45:23</p> <p>literally 39:21 45:19</p> <p>litigating 29:21</p> <p>litigation 51:2,12,19 56:7,20 57:10,22 65:18,19 71:1,7 93:11,16,25 105:20 116:9 249:13</p> <p>little 7:3 16:18 17:23 28:18 33:2 43:23 55:23 58:10 74:14 76:20 77:19 82:22 95:1 101:15 114:12 116:23 132:3 140:25 142:24 143:16 151:11 153:5 155:20 160:25 170:23 174:14 175:14 190:10 201:25 202:2 207:14</p> <p>live 23:10 43:6 45:18 112:20 114:4 115:15,21 138:12 139:4 140:17 141:11,24 143:19 144:5,6,11 150:18</p> <p>lived 112:21</p> <p>livelihood 42:1</p> <p>lives 35:20 125:21 152:13 210:22 227:5</p> <p>loads 256:2</p>	<p>loathe 260:21</p> <p>location 59:3</p> <p>lock 50:6 54:17 74:9,18 84:24 98:5 110:8,11,13 113:7 221:9</p> <p>locked 215:1 235:6,9 240:2 257:16</p> <p>locking 212:19 213:2,6</p> <p>lock-picking 50:4</p> <p>locks 38:12 50:3 54:10 73:9,10,17,19,25 74:14,21 113:9</p> <p>locksmith 231:19</p> <p>logjam 36:4,18</p> <p>long 17:2 21:9 35:7 43:20 48:6 69:23 71:6 84:5 108:21 109:3,7 124:2 189:10 195:3 210:2 221:3 243:16,17 244:13,16,18 247:15,23 248:3,4,19,25</p> <p>longer 162:20 176:23</p> <p>loomed 72:24</p> <p>loose 86:9</p> <p>Los 5:10 6:19</p> <p>lose 181:7</p> <p>losing 24:21 160:24</p> <p>loss 34:2</p> <p>lost 60:24</p> <p>lot 17:17 21:5 27:16 34:4 52:14 69:7 84:14,17,19 88:7,23 92:5 94:21,22 105:21</p>	<p>129:21 130:14 131:17,21 140:16 144:8 147:2 155:9 169:14 171:11 176:8 185:9 196:3 197:19 198:23 223:13 228:17,18</p> <p>Lovells 9:17</p> <p>low 20:2 155:7</p> <p>lower 223:24</p> <p>luck 112:9</p> <p>lying 173:23</p> <hr/> <p style="text-align: center;">M</p> <hr/> <p>machine 161:18 162:2,9</p> <p>machines 161:20</p> <p>Mackey 208:21,25 209:8,9</p> <p>mail 257:8</p> <p>mailbox 39:22,24 137:25 151:11,14</p> <p>mail-order 256:22</p> <p>main 202:6 251:4 255:13</p> <p>mainly 57:14</p> <p>maintain 178:13</p> <p>maintained 15:11 26:25 128:10</p> <p>major 62:11 140:7 158:20 160:13 164:2 172:6</p> <p>majority 34:7 142:5 189:2</p> <p>maker 50:6</p> <p>malefactors 126:4</p> <p>malicious 96:11,14 97:4 171:6</p>	<p>Malone 210:5,13</p> <p>managed 102:17</p> <p>management 58:2,22 60:3 178:9</p> <p>manages 102:18</p> <p>mandates 232:2</p> <p>manner 15:11 27:1 126:3 128:10 129:10 130:25</p> <p>manufacture 74:15</p> <p>manufacturer 11:15,23 12:5,6,7,13 52:5 54:9 58:21 78:21 80:10 82:19 87:7 121:12 130:5 153:10,13 174:2,3 231:12</p> <p>manufacturers 34:5 52:1 69:7 77:12 82:16 121:4 135:12 158:9,11 175:4</p> <p>marginally 48:12</p> <p>Mark 8:20 39:10</p> <p>marked 54:3 123:19,21</p> <p>market 76:3 129:4,5 130:19 163:17,24 164:3 175:24 181:9 188:21 190:17,19 192:4 240:16 241:10,18 259:8,9,24</p> <p>marketplace 97:16 98:4 173:1 238:20</p> <p>marketplaces 239:2</p>
--	---	---	--

markets 175:19 180:12,24 187:22	may 1:7 14:7,8 20:5,6 25:22 34:12 40:20 43:18,19,20 44:11 46:9 51:14 53:19 61:23 62:22 64:3,10,12,22 69:8 70:3 80:15 92:14 101:25 106:25 107:24 110:1,10 115:22 118:25 120:7,8 121:3,4,5 125:23 131:13 140:18 141:6 143:24 147:12 153:12 159:13,15 174:24 175:3 176:8,14 184:1 191:15 205:17 207:11,19 212:9 218:13 222:3 228:25 231:14,19 232:18 242:16 243:23 246:9 250:9 254:23	67:19,20,21,24 68:5,25 69:5 82:15,17 85:24 86:6,9,16,19 88:2,20,21 89:8,10 102:15,23 103:8 104:24 105:16 106:24 107:10,13,18 108:9,12,20 111:8,15 112:6,11,15,24 113:6 114:11 115:13,19 118:7 129:21 130:3,10 132:3,4,22 133:5 136:15 138:5,9,11,13,16 ,23 139:19 140:12,13,21,23, 24 141:4,8 142:16,19,20 143:6,17 144:2 150:7,16 164:16,18 165:14,22,25 166:21 167:13,23 168:3,15 169:7,9 170:5,16,18,22 171:2,7,19 172:3,17,23 174:14,17 175:6 176:17,24 177:5 179:19 183:5,12,16 184:17,21,22 185:22 187:14 188:16 190:8,11,17,24 191:8,12,13,22 192:12 201:25 202:1 203:6 210:14 214:12 218:12,18,21 220:1,4,20 221:12,13,19 223:12,13,17 224:14,16	225:22 226:2,3 227:22 228:1,14,17,23 229:4 236:18,20 239:19 240:25 243:5 248:16 250:6,21 254:21 259:12 meaning 81:13 118:7,9 216:4 242:5 meaningful 182:20 212:13 meaningfully 184:14 meanings 118:19 means 6:23 14:4 31:13 53:17 67:22 131:1 157:24 177:8 212:23 214:17 216:21 249:5 meant 240:16 252:14 meantime 163:24 174:6 measure 13:23,24 145:6 147:16 measures 26:13 48:21 120:13 134:7 148:11 186:21 194:25 mechanical 73:8,9,12 74:2 75:4 mechanically 74:22 mechanism 53:6 62:18 66:19 189:23 204:14 mechanisms 200:7 mediate 84:13 mediating 190:4 medical 22:22
Markey 70:8			
mass 80:24 81:25 82:10 114:2,6 115:4,17			
massive 83:7			
master 73:10,16,25			
MasterCard 10:8			
material 147:10,20 148:4 149:2			
materials 166:9			
Matt 9:3 117:1			
matter 54:23 55:4 58:16 102:3 130:11 144:21 147:6,14 148:22 159:18 224:20 237:10,11			
Matthew 8:1 9:24			
Matwyshyn 8:24 50:16,18,20 52:21 54:4 55:17 56:10 57:17,24 58:12 59:1,19 60:8,13,17 61:7,13 62:22 63:24 64:2,12 65:6,12 66:10,17 67:1 68:18 69:12,25 70:3,24 84:15 92:12,13 149:5,6,18,25 158:2,3 186:18,19 187:8,16,20 188:14,18,21 190:18,22,25 191:3,10,14,19,2 3 192:5,8 193:7 198:19 199:7 200:4 201:4,7,9 202:4 203:13	maybe 6:1 29:16 30:7 77:20 80:21 83:11,18 86:10,16 87:10 114:8 116:1,3 141:12 143:16 157:3 170:19 174:22 175:7 176:19 177:6 184:24 190:11 207:10,14 216:15 217:20 243:9 250:8 mean 12:5 16:23 17:1,3 27:9 28:9,12,20 29:9,18,19 30:3,14,22 31:3 33:5,10 36:18 51:22,24 52:13 64:6 65:25 66:1		

<p>26:7 35:21 36:15 103:18,21 144:11 198:25 meet 23:18 44:10 226:6 meetings 91:3 135:2 member 35:3 93:6 131:15 132:21 233:4 236:13,14,16 237:7 members 34:21 89:7 125:6,8,11 132:4,16 225:11 238:16 239:4,15 241:5 243:25 247:2 251:9 252:23 membership 230:4 memo 91:16 memory 25:22 mention 48:17 57:20 113:25 mentioned 4:4,16 5:10 12:4 28:6 36:17 37:19 38:8 40:22 49:12 53:14 68:20 70:9 87:14 135:22 144:7 168:13 175:19 201:11 234:10 246:10 mentioning 85:25 merely 56:19 127:15 152:2 merits 13:6 message 40:11,14 116:23 messages 39:15 41:4 met 152:14 metes 109:10</p>	<p>method 89:10 181:24 Michelle 2:3 4:19,20 206:20 microchip 174:23 Microphone 8:4 microphones 45:23 Microsoft 101:21 157:13 middle 185:15 midst 126:7 mike 6:24 8:7,12 54:1,5,13 55:22 209:16 mikes 6:17,21 Mike's 54:7,19 miking 6:16 mileage 28:22 Millennium 57:21 Miller 33:24 192:17 million 96:21 176:2 millions 25:7 121:3,10 176:22 230:8 mind 32:13 88:15 94:14 mindful 129:11 mine 75:7 90:21 91:9 227:7 minimum 20:19 minute 124:6 196:3 minutes 155:18 177:17 197:9 mirrored 159:20 misleading 173:17 mistake 140:23 misunderstood</p>	<p>190:17 misuse 227:24 misusing 227:23 mitigate 10:19 20:13 38:20 51:12 80:11 mitigation 186:21 mitigations 11:20 Mm-hmm 60:8 65:6 66:10 69:12,25 79:20,22 103:25 104:5 106:15,18 112:2 130:1,10 133:1 164:6 165:16 167:15 184:19 201:4,8 234:8 236:15 237:15 251:14 mobile 45:19 212:7,12 245:17 246:6 model 53:11 66:14 183:2 241:7 modeled 212:3 models 184:2 212:10 213:22 219:19 259:20 modern 43:6 modifications 232:13 modified 232:12 modify 110:21 MOLARO 263:2,18 moment 13:2 106:7 143:25 179:16 monetary 44:19 money 66:2 96:18 196:3 210:22 monitor 194:13</p>	<p>monitoring 194:5 month 49:18 156:18 233:16 monthly 219:17 220:3 223:25 months 96:19 163:22 188:8 Moreover 20:18 23:2 morning 4:2 21:2 34:19 39:10 133:16 138:1 Mostly 160:14 motivating 137:8 Motors 9:15,17 mouth 235:3 move 34:18 94:11 109:19 229:20 243:11 moved 84:9 moving 198:25 199:15 215:16 245:11 Moy 9:6 23:21 94:13,15 100:13 163:12,13 164:6,13 165:16,22 167:6,15 168:4 169:4,6,9,12,19, 21 170:1,3 171:19,21 172:23 173:7 179:20 197:21 multifactor 15:4 29:15 multimedia 7:9 multiple 54:14 118:3 155:19 156:7 Mumford 1:9 mundane 52:12 murkiness 58:13</p>
---	--	---	--

122:18 murky 58:11 150:24 207:14 music 22:18 myself 10:23 20:13 74:6 109:6 159:8 162:3 166:1 172:12 175:1 <hr/> N <hr/> naive 11:13 20:8 namely 128:21 narrow 26:9 27:18 120:19 127:15 136:17,23 narrowed 132:25 narrowing 136:6 143:13 nation 39:2 national 23:15 37:9 129:12 161:6 230:7 nationals 159:24 nation's 23:5 25:6 126:1 230:2 nature 33:7 141:14 163:18 164:17 167:10 168:8 187:11 199:9 203:19 231:22 navigate 76:17 Nearly 127:4 necessarily 18:10 27:15 102:24 104:12 171:4 174:19 175:24 176:5 233:16 235:7 237:11 261:3 necessary 19:10 20:22 85:5 115:22 143:24	185:6 231:20 250:4 neglected 135:20 neglecting 25:10 negotiated 68:21 69:4 250:15 251:1 252:7 negotiation 84:15 negotiations 84:17 neither 262:10 263:4 nephew 217:23 218:5 227:5 236:17 nervous 17:17 net 38:14 network 101:6,24 102:4,16 108:5 111:20 116:20 128:6 171:1 212:25 217:6,11 221:12 226:1 230:24 231:7 232:16 242:8 249:7,16 250:24 257:17 network- connecting 212:18,22 213:6 networking 22:23 networks 108:16 210:21 230:12,15,23 nevertheless 65:17 newcomers 206:12 newest 217:24 news 140:13 168:17 new-to-the-world 49:16 nice 57:4 Ninety 155:7	nobody 89:25 150:19 159:18 nodding 124:8 nods 258:16 noncopyright 248:10 noncritical 114:16 none 127:22 Nonetheless 74:9 noninfringing 38:25 202:19 230:16 nonsoftware 197:1 nontrivial 72:25 nor 262:10,14 263:4,5 norm 78:13 79:24 80:19 153:18 normally 162:11 norms 149:21 187:4 198:20,23,24 Notary 262:1,19,23 note 55:12 56:14 211:1 247:11 250:14 noted 37:7 92:18 120:22 122:1 212:11 nothing 27:24 50:10 145:3,6,7 212:12 226:24 notice 162:9,13 166:24 196:9 245:21 noticed 189:8 229:13 notification 94:24 159:7,8 notified 11:15	82:9 163:3,4 179:4,10 notify 63:25 80:25 81:3,9,16,21 82:16 83:8 130:5 154:15,17 155:4 162:23 notifying 41:24 44:15 81:11 82:3,19 83:19 142:25 162:18 noting 22:1 133:17 notion 69:12 205:6 241:2 notwithstanding 153:11 NTIA 5:6 21:7 34:21 207:6 nuanced 68:14 nuclear 114:1,5 115:15 138:5,13 140:8 141:14 nudge 63:15 93:18 192:8 numerous 36:14 42:18 44:19 nutshell 214:2 254:19 <hr/> O <hr/> Obama 126:18 246:17 object 70:10 224:15 objected 221:18 239:11 objecting 222:7 objective 64:7 126:2 obligation 154:23 220:22,23 236:1 244:11 obligations 221:8
--	--	--	---

<p>234:5,22 235:8 237:19,20 243:22 244:7 obscure 184:13 obstacle 45:12 obstructs 212:20 obtain 128:4 225:9 239:5 obtained 128:3 217:4 243:4 250:6 obviously 6:20 33:10 44:2 51:25 60:10 79:2 96:5 119:2 130:16 138:14 139:6 145:22 165:18 237:1 occasions 54:14 occupants 134:5,10 occurred 41:23 194:6 OCR'd 49:15 odd 151:11 159:20 offer 41:11 222:2,3,4 223:23 254:8 offered 44:6 227:3 259:21 offering 130:22 offhand 156:18 office 1:5 2:2,4,5,7,8,10 4:9,21 15:22,23 16:9 21:7,13,16,21 22:7 23:3,12 25:1,11 34:21 35:13 38:22 84:20 95:7 100:17 112:17 116:6,13 117:21 119:16,22</p>	<p>122:20 136:5 138:16 145:14 199:4 206:16,21 212:1,11 231:1 233:23 245:21 256:13 officer 262:2 officers 75:17 offices 73:10 office's 142:11 232:2 official 132:10 off-the-shelf 115:9 oftentimes 114:14 oh 34:18 50:19 119:24 155:14 156:2 157:3 166:23 oink 40:9 okay 5:7 8:10 9:20,24 12:8 14:11 18:15 19:5,8,11,15 26:14 28:2 30:12 32:3 34:17 37:3 39:7 40:19 43:14,18,24 46:15 53:22,23 58:8 60:16 61:1,21 66:21 70:22 71:14 80:10 90:7,12 94:4 109:3,16,18 110:3 119:24 121:15 123:12,20 124:2,14 132:15,22,24 133:11,14 136:17 137:5,19,21 142:1 146:6 149:4 150:7 155:13 156:2 157:9 158:1 160:5 163:11</p>	<p>168:10 169:25 173:6 174:9 176:19 177:16,17 184:16 186:16 187:18 190:8 195:6,8 196:25 198:5,18 203:12 204:2,9,10 205:10 207:8,10 209:1 210:14,15 215:16 216:9,14 220:8 224:13 225:2 229:19,22 232:21 235:1 236:8,11 237:23 242:14 243:8,13 244:14,19 248:24 249:19,24 251:5,22 252:5,13,22 253:6 255:5 256:6,18 258:22 260:2,3 261:8 old 217:21 218:8 220:5 224:8 227:14 one-line 57:4 ones 30:24 31:4 47:17 166:18 194:15 219:23 220:5 252:17 one's 245:11 online 49:14,15 139:13 onto 205:8 245:11 256:25 open 9:7 50:7 73:11,16 120:25 201:12 229:24 261:4 opened 201:23 opened-ended 129:25 opening 5:23 7:23</p>	<p>90:8,9,12 124:21 207:16 208:15 209:7 openings 158:13 open-source 34:8 operate 11:6 140:24 operates 102:22 operating 48:9,12 138:7 140:17 operator 15:8 26:24 83:20 101:5 102:15,20 103:3 109:5 111:19 170:25 operators 103:6 opine 17:3 opinion 12:23 50:11 199:8 opinions 147:13 opponent 31:9 232:10 opponents 60:4 95:10 opportunity 25:1 46:18 70:10 71:16 94:10 100:10 122:20 123:8 125:16 129:1 135:13 152:23 205:21 226:23,24 oppose 127:16 opposed 80:3 158:18 250:19 opposes 247:12 opposition 95:17 124:7 211:1,3 232:9 option 259:7 options 98:5 172:24 order 7:3 31:2</p>
--	--	---	--

<p>45:24 49:10 75:24 76:5 119:14 147:3 148:9 155:22 169:2 175:9 185:2,3 216:23 230:23 239:3 ordinarily 162:12 ordinary 73:15 148:13 165:21,22 166:21 167:2 216:20 255:17 256:3 organization 178:4,20 201:14,17,24 organizations 20:16 44:20 156:6 origin 253:24 original 37:20 91:16 231:25 233:10 234:4,5,22 235:7,17 236:1 237:18 242:21 243:21 244:3,6 252:12 253:12 256:11 originally 230:25 253:16 others 32:12 35:15 50:6 63:5 72:10 75:11 86:13 96:6 98:2 131:24 135:2 166:8,9 171:22 182:14 185:4 186:6,7 213:25 216:13 254:4 256:25 otherwise 149:2 166:16 262:15 ought 98:6 144:14 ours 93:12 257:24,25</p>	<p>ourselves 210:24 outcome 56:4 161:11 262:15 263:5 outlet 249:15 outlets 168:18 outlined 31:16 55:13 outright 179:9 outset 21:6 32:14 outside 104:12 106:8 159:16 outstanding 21:5 outweigh 177:13 outweighed 162:17 oven 45:20 overall 112:23 134:13 243:10 overarching 113:11 overflow 47:5 overhears 45:25 overheat 194:22 overlap 188:12 overlapping 69:16 overlooked 98:10 overly 124:3 overriding 23:15 137:6 overseen 33:7 oversight 172:7 Overstock 256:24 overzealous 53:17 owned 121:12 owner 15:8 26:24 101:5,16,17 102:4,15,20 103:3 104:2,13 105:3,12 111:19</p>	<p>117:2,15 128:5 170:25 213:10 233:11 234:4 235:4,8,17,21 236:1,6,18 237:18 242:22 243:21 244:3,4,6 251:6 253:12 256:11 257:25 260:25 owners 44:4 103:6 235:23,24 236:8 237:17 238:19 244:10 245:17,23 246:4,5 253:14 ownership 213:16 owns 68:1,3 102:24 106:22 117:9 120:20 <hr/><p style="text-align: center;">P</p><hr/>p.m 261:20 P25 75:8,13 pacemaker 103:23 104:3,22 package 218:3 page 3:2 49:25 50:5 60:1 196:17 paid 196:3 palpable 133:4 panel 14:21 32:13 36:21 43:20 50:21 51:18,23 62:24 93:1 124:3 199:19 205:11 206:5 219:6 panelists 100:24 paper 83:4 90:20 91:9 110:4 papers 114:1 135:21 136:16 186:5,10 paradigm 65:13</p>	<p>paragraph 55:3 90:23 paragraphs 91:11 229:25 parallel 258:14 parameters 76:16 parent 40:13 151:16 parents 39:15 partake 69:4 partial 50:10 participants 5:23 158:21 participate 69:8 135:1 178:21 participating 199:20 208:24 participation 137:8 particular 7:7 31:10,11 35:16 54:16 62:25 63:14 73:9 76:7 78:20 95:10 104:3 120:20 121:1 125:12 133:13 142:5 159:2,4 162:10 170:14 188:23 193:16 226:5 228:23 233:25 236:23 237:7 257:17 particularly 6:6 77:25 85:17 103:1 131:14 134:16 205:14 254:6 260:23 parties 38:1 91:17 101:9 126:10,11 172:8 229:7,10,20 262:11,14 partly 151:5</p>
--	---	--	--

partnering 130:20	45:13 52:9,14	perhaps 11:18	228:7,11 253:20
party 106:12,22	62:4,7,11,12	64:23 86:17	perverse 180:10
109:5 159:16	66:3,15 68:7	110:21 120:2	Peters 23:25
211:3 231:22	81:3,6,9 82:3,9	159:25 172:10	petition 38:22
239:10 247:12	83:19 92:2,5	198:20 207:19	211:19
263:4	108:15	212:6	Petitioner 245:2
pass 60:25 218:5	113:15,20	period 89:23 93:4	petitioners 8:3
259:10	116:14 123:7	217:17 221:2,6	9:11
passed 73:1	124:4,8 127:9	232:8 260:23	petitions 231:1
passing 224:11	139:12,23	permeate 70:18	ph 23:25
past 15:23 90:11	143:4,13 150:5	permissible	Ph.D 47:25
117:21	157:20,21	110:6,7	phase 77:14
119:16,22 136:5	165:23 166:15	permission 43:22	phased 211:22
217:2 224:23	167:20	201:24 254:8	Phil 210:5
259:19	168:19,21	permit 128:2	phone 28:10 45:19
patch 131:2,18	174:20,23	221:15 232:15	48:21 102:8,10
155:5 174:6	176:14,19	239:13 249:3	104:22 157:4
175:18	182:22,23 185:4	permitted 247:9	213:8,14 214:23
patched 82:13	186:14	permitting 50:21	215:1
129:2 189:5,8	188:9,13,17	pernicious 23:4	217:1,3,14,16,18
patches 131:16,23	190:13 192:12	persist 22:18	,22,24
patching 163:25	205:5 206:2	persisted 21:9	218:1,3,9,11,18
path 18:24 243:10	215:18 221:20	person 41:1,3	219:8
patient 94:11	222:11 226:7	78:15 101:11	220:2,9,15,19,22
199:1	227:23 239:25	102:18,19,21,23,	221:9,11,14,22,2
patients 198:25	260:18	24 103:2 104:18	3 222:21
patronize 97:10	people's 152:12	106:3 110:10,13	223:7,10,16,18
pause 59:25	165:4 178:14	115:1 140:22	224:8,9,11
179:16	perceive 140:19	185:17 208:22	225:15,16 226:4
pay 220:9,20	percent 83:12,14	228:15 231:17	227:9,11,14
223:10 224:9	155:7 185:15,17	personal 38:19	233:5,6,12,14,17
225:17	percentage 132:5	42:8 70:10 96:20	,24 234:18,25
234:11,21	perception 41:21	98:14,20 99:1,4	235:5,6,9
payment 11:7	perennial 228:1	159:14	236:7,13 237:2,3
219:17 220:3	perfect 140:22	personally 49:21	239:14,16
pays 234:15	perfectly 213:19	92:3 188:6	241:14 244:4
pedophile 43:2	perform 109:12	personnel 53:7	245:11,23
penniless 13:3	141:13 231:18	158:13	246:25 247:1
Pennsylvania 9:5	performed 27:7	persons 127:2	248:1 249:3
71:19	87:24	perspective 56:16	250:23 251:8,12
people 11:9 14:2	performing 35:11	59:1 60:13,17	252:22
27:21 29:1 33:18	38:5 99:7 107:6	67:3 69:18 73:21	253:12,16,24
	139:3 140:9	170:11 187:23	255:16
	183:8	200:11 216:20	257:5,7,15,16
	performs 189:18		259:10,15

<p>phones 35:20 215:24 218:16 222:11,12 223:1 224:20,21,24 225:9 228:19 238:16,18,19,24, 25 239:5 240:1,9,16 241:6,11,16 244:2 245:19 246:5 247:3 249:4,5,8,14,17 252:15,16 256:22 259:21</p> <p>photograph 43:20</p> <p>physical 147:8</p> <p>pick 106:14</p> <p>picture 41:7</p> <p>piece 7:7 14:9 25:23 26:3,5,9 32:1,17 52:18 59:2 176:23 195:22 200:12</p> <p>pieces 26:2</p> <p>pig 39:20 115:2 151:12,15 153:5 155:16 157:6 167:19,20 198:11</p> <p>piggy 137:25</p> <p>pilot 141:7</p> <p>piloted 141:6</p> <p>piloting 141:7</p> <p>pink 153:5</p> <p>placard 7:1 34:24 177:20 208:9</p> <p>placed 38:23 59:3 128:20</p> <p>plaintiff 57:7</p> <p>plan 233:7</p> <p>plane 138:7 141:4 198:24</p> <p>plane's 138:6</p>	<p>planned 254:15</p> <p>plans 240:17</p> <p>plant 115:16</p> <p>plants 114:1,5 138:5,13 140:8 141:14</p> <p>plastic 39:20</p> <p>platform 41:6</p> <p>play 40:11 100:8 134:13 190:23</p> <p>played 27:21 72:22,23</p> <p>Please 46:1</p> <p>pleased 210:18</p> <p>plug 196:16</p> <p>pockets 35:20</p> <p>point 16:19 17:20 29:13 30:4 36:3 42:2 47:3 48:2 56:20 61:3,8 63:6,10 64:9,13 67:4,7 69:14 70:16 78:23,24 81:20 92:20 93:4,5,10,24 95:23 100:24 102:23 106:19,25 107:1 109:15 110:5 112:11 115:7 116:4,8 118:16 121:18 122:7 150:24 153:6,23 154:23 155:18 156:23 158:4 175:13 179:5 187:21 189:15 194:17 195:13 197:22 202:11 204:12 207:12 216:16 234:24 235:21 241:25 242:17 246:9 251:6 253:10</p> <p>pointed 96:6</p>	<p>194:11</p> <p>points 61:9 69:15 92:13 99:19 100:21 179:1 181:18 187:21 234:7 245:4 248:7</p> <p>poised 215:6</p> <p>policies 66:15 146:1 159:12 214:10,15 215:5 221:20</p> <p>policy 8:15,18 9:7 35:4 70:17 85:17 95:9 126:19 129:12 144:22 145:13 159:14,19 171:2 189:16 205:8 209:15 215:10 221:15,20</p> <p>poll 198:6</p> <p>poorly 113:3</p> <p>portion 245:6</p> <p>portions 149:13</p> <p>positing 108:2 222:15</p> <p>position 55:10 62:15 81:10 93:17 106:3 116:14 136:15,21 224:25 250:8 251:16,21 260:22</p> <p>positioned 187:9</p> <p>possess 41:16 53:13</p> <p>possessing 43:4</p> <p>possession 147:9 188:1</p> <p>possibility 13:4 43:2 150:22 254:24 255:8</p>	<p>possible 20:12 34:12 44:23 74:8 76:13 82:4 97:2,14 118:1 125:2 154:12 182:8 183:15,19 213:2 257:4</p> <p>possibly 13:5 44:3 45:18 47:21 147:7</p> <p>post 174:15,21</p> <p>post-hoc 28:24 29:7 30:8</p> <p>posture 56:9 70:2</p> <p>potential 57:7,21 84:1 103:6 118:11,13 125:4 143:12 179:2 180:15 216:23 231:5 239:7</p> <p>potentially 14:4 106:2 168:19 175:17 188:7 196:14</p> <p>pounce 96:14</p> <p>power 114:1,5 115:15 138:5,13 140:8 141:14 205:8</p> <p>PowerPoint 53:19</p> <p>practical 47:14 138:10 224:19</p> <p>practice 27:21 158:23</p> <p>practices 58:2 88:23 98:13,25 99:17 100:5 125:23 172:5 187:3,15</p> <p>practicing 38:25 177:8</p> <p>pragmatic 147:6,14</p> <p>preceded 100:21</p>
---	---	--	---

preceding 96:19	84:11 86:20	162:3	76:19
precise 247:21	147:17 260:18	prizes 44:20,21	proceeded 77:16
precisely 107:20	prevent 12:14,24	pro 18:4 20:15	proceeding 9:19
146:11 160:20	139:23 148:19	probability 20:1	16:2 22:11 95:18
214:1	189:12 226:9	81:22 83:9,20	96:10 116:11
predecessor's 45:3	prevented 14:8	155:6	125:3 126:2
predictable 29:17	45:7	probable 148:6	134:23 137:9
predicted 22:3	prevention 13:23	probably 32:11	143:15 144:4
prediction 24:1,8	174:1	33:2 42:19 51:23	187:24 206:13
prefer 214:24	prevents 213:13	52:14 63:21	209:4 231:8
preferential 254:3	previous 33:22	64:21 67:8 81:18	250:20 252:10
preliminary	36:12 214:25	82:8 131:25	254:9 261:6
130:11	previously 26:4	132:11 138:2	process 5:12 44:12
premarked 7:12	30:24 123:7	164:14 174:23	58:23 60:3 61:10
prepared 6:3	181:5 217:10	194:8 202:23	63:15 69:10
207:22 263:3	price 223:24	206:2 215:7	100:2 150:4
prescient 24:9	228:20 240:3	221:22	152:1 179:19
presciently 70:14	243:24	probative 87:16	182:2 186:4
prescriptive 84:20	primarily 26:23	problem 43:25	188:6 199:17
present 77:7 80:14	28:8,13,24 29:3	62:8 63:10 65:5	214:22 249:9
134:8,9 149:11	36:23 77:4 92:17	82:25 91:25 93:9	261:21
188:3 230:18	116:22 128:9	105:19 106:1	processes 53:5
presentation	primary 198:13	107:13 111:9,12	60:7,12,22
238:11	246:20	113:15 121:14	61:5,15 64:9
presented 134:17	Princeton 8:25	125:17 128:22	67:8 158:7,9
173:18 180:5	principally 126:17	150:2	186:24 200:6
presenting 13:3	principle 252:21	164:1,10,14	processors 238:14
preserve 111:6	principles	166:23 168:18	pro-consumer
160:20	178:12,13	170:3,17 179:3	245:10
President 211:23	printer 90:22	182:25 183:3,7	product 47:6 52:6
245:9 246:17	prior 45:5 55:24	185:3 188:9	54:12,18 78:20
presiding 4:10	71:25 85:12	196:15,18	80:9,16 98:8
press 97:25 146:2	priority 23:15	200:22,23 202:8	163:18,20,24
pressure 194:4,13	privacy 35:1 44:3	problematic 22:4	165:12 189:7,8
197:21	45:8 46:4 70:11	28:25 78:1	200:14,17
presumably	94:21	problemized	production 46:13
103:9,11,21	95:1,12,14,15,16	203:18	productive
220:19	,19 96:4 178:12	problems 142:9	4:13,15 41:22
presumptively	189:16	179:10 189:24	products 38:3
232:7	private 32:22	190:1 196:7	46:12 53:3 55:6
pretty 31:17 51:23	33:18 34:8 92:8	203:16 228:8	74:10 75:15
	126:11	254:5 259:18	76:1,9 79:8,14
	privy 42:12,20	procedural 162:16	97:10,15 98:19
		procedure 231:18	114:23 151:9
		proceed 19:6	157:16 179:25
			200:18

profession 84:6	53:1 132:13	57:14 58:5	110:13 121:13
professional 10:6,12	progress 156:22	59:22,24 108:7	134:7 148:10,12
Professionals 209:17	prohibited 223:5	109:10 110:18	149:2 213:7
professor 7:24	prohibition 212:8	132:25 215:23	216:23 247:5
8:2,23	prohibitions 127:7	232:24 243:18	protecting 42:24
9:2,4,22,25	prohibitive 57:2	252:8,12,14	47:17 82:3 83:18
10:4,6 14:13	project 11:10,11	254:3 255:25	98:14 117:7,8
15:15 16:13,20	16:1 18:17	proposals 94:23	147:17 153:21
17:14 18:25	20:10,21 33:7	126:9 130:4	protection 13:24
20:25	proliferation	253:19 258:7,9	26:13 113:17
21:1,14,15,21	22:14	propose 212:3	134:7 145:6
22:12 23:4,19	prominent 100:7	227:21 256:13	147:15 152:21
24:1,8,17 29:1	prominently 59:3	proposed 3:3,4 6:9	193:17 213:12
32:12,18 33:1	promised 13:10	26:19 35:9,13	231:3 257:25
35:6,8 36:1,20	promises 98:16	56:2 57:16 68:19	protections
37:7 38:8	promising 255:11	70:21 71:15	231:24
46:16,19 47:20	promote 15:8	94:19 95:2	protective 120:13
50:15,16 61:3	26:23 126:3	108:19 116:7	protects 13:25
62:23 63:1,12	127:7,14 128:9	127:18 133:19	232:24
70:23	170:24	135:11 208:12	protocol 36:5
71:13,18,24	prompt 44:13	209:12 210:18	protocols 75:19,22
80:21 84:8,15	prong 67:10	211:2,4 226:7	prototypical
92:12 93:22 94:6	pronouncement	229:14,15	101:18
118:17 119:25	261:2	230:25	prove 216:22
120:2,22 121:16	proof 173:20,24	232:1,11,12	provenance
124:21 144:6	216:21 217:12	234:20 238:7	253:23
146:7 149:5	254:5 255:15	239:12 242:18	provide 15:1
150:15 153:24	256:3	247:24 249:1,18	16:10 18:6,13
154:8 155:14	proper 49:23 50:3	250:3 257:4	23:16 28:16
158:1,2 159:5	properly 140:10	261:16	31:14,24 58:5
160:23 161:2	154:19 177:4,9	proposing 70:8	62:24 70:9 86:2
166:5,6 181:15	212:18 232:14	112:12	93:2 97:14 119:1
186:17,18	property 51:6,7,9	props 39:8 213:21	130:24
193:6,7,9,22	110:13 117:8	pros 224:2	154:11,21 167:9
195:11,13	186:4	prosecute	231:14 232:6
198:1,19 203:12	proponents	179:22,23	provided 18:4
204:8,11,16,17	124:17	protect 23:21 25:7	57:24 59:9,10
210:5,13	127:11,15,19	51:6 83:11,14	62:19 102:23
profit 125:20	128:24 134:17	90:3 97:5 98:20	200:15 243:23
profited 49:22	152:14 239:12	120:6	provider 103:10
program	proposal 5:25 27:4	144:16,17,25	231:17
48:7,10,16	28:11 55:13	148:17 160:21	providers 157:18
programming		174:5 176:22	230:3,5,6,7
48:17,18		178:1,14 185:5	provides 57:4
programs 48:25		247:1	93:12 154:1
		protected 14:8	
		18:8 23:20 48:20	

<p>238:21</p> <p>providing 9:18 94:1 113:12,17 131:1 186:13</p> <p>province 84:5</p> <p>provision 77:21,25 101:2 109:13 145:9 247:16</p> <p>provisions 12:19 17:18 26:19 96:2 97:7 113:3 122:8 127:16</p> <p>prudent 80:15</p> <p>public 10:14 11:10 13:8 20:1 36:24 38:2 50:9 52:7 62:17 67:3 79:5 80:15 81:4,22 83:22 89:7,17 91:23 93:20 97:22 128:25 131:4 138:22 142:25 151:21 154:3,5 156:20 163:10 165:2 175:9 176:6,20 182:1,4 189:13 191:17 201:6,13 209:10 211:22 238:22 261:21 262:1,19</p> <p>publication 78:16 80:3 90:19 159:11,17 160:7,8,18 163:22 181:4,12</p> <p>publicized 164:22</p> <p>publicly 31:21 66:18 82:20 91:6 92:9 173:18</p> <p>publish 12:1 20:4 74:16 78:10 90:4 91:14 113:21 168:17 181:22,23 184:17 186:5</p>	<p>publishable 47:7</p> <p>published 20:3 74:5 75:19 91:10 163:3</p> <p>publisher 49:16</p> <p>publishing 12:15,25 31:10 138:18 166:13 193:1</p> <p>pulled 173:13</p> <p>pulling 194:23</p> <p>punt 243:9</p> <p>purchasable 115:10</p> <p>purchase 97:10 98:8 104:19 115:12 225:15 239:1 241:14 257:1</p> <p>purchased 148:19 212:15 213:15</p> <p>purchaser 251:8</p> <p>purchases 104:22 188:23</p> <p>purchasing 165:11</p> <p>purely 56:25 73:11 74:2 75:4 146:20</p> <p>purport 133:20</p> <p>purpose 28:12,13,14,17 29:3 35:10 89:13 108:21 128:7 151:4,8 193:20 199:11 211:12 213:3 243:3 251:25 252:11 255:17</p> <p>purpose-built 133:23</p> <p>purposeful 216:4</p> <p>purposes 140:19</p>	<p>141:10 200:15 202:19 252:2</p> <p>pursuant 232:19</p> <p>pursue 26:11 78:7 161:23</p> <p>pursuing 157:5</p> <p>push 117:25 118:20 201:12</p> <p>pushback 11:23 177:1 179:8</p> <p>puts 81:5</p> <p>putting 45:14 93:16 106:2 178:19 250:12</p> <hr/> <p style="text-align: center;">Q</p> <hr/> <p>quality 50:7 200:16</p> <p>quarterly 178:7</p> <p>question 26:17 27:12 29:5,19 32:4 46:9 50:11 51:2,21,22 58:15,17 60:19 63:14 80:5 83:3 85:3 89:11,19,22 101:13 105:9 106:11 108:1 114:8 116:1,19 117:9 120:20 135:19 138:17 139:20 141:12 144:14 162:8 164:5 168:5 176:18,25 184:17 194:17 198:7 203:14 215:22 228:5,11 239:19 240:15,25 247:24 249:20 250:2,4 254:25 258:3 260:4</p> <p>questioned 190:10</p> <p>questioning</p>	<p>121:20</p> <p>questions 5:14 6:3 21:4 25:15 39:6 46:7 51:10 70:25 71:10 100:12,23 107:24 129:18 190:7 205:18 207:15,22 211:15 214:8 254:23 256:19</p> <p>quick 184:17 187:20 188:4 204:12 248:7 256:8</p> <p>quickly 7:19 163:14 181:5 198:6 202:11 203:13</p> <p>quietly 41:23 44:15</p> <p>quite 5:22 43:9 90:2 150:24 151:10 155:1 180:21 190:6</p> <p>quote 24:3 246:21</p> <p>quoted 173:16</p> <p>quotes 56:21</p> <hr/> <p style="text-align: center;">R</p> <hr/> <p>race 24:22</p> <p>racing 96:15</p> <p>radio 75:9,12,15,16 76:1 133:25</p> <p>rails 61:11 67:6</p> <p>raise 12:17 201:12</p> <p>raised 14:10 100:24 144:9 145:23 158:4 179:1 228:24 235:2</p> <p>raising 100:23</p> <p>rallying 149:14</p>
--	--	---	---

random 108:5,6	realized 77:14	received 18:19	262:6
range 36:11 44:8 80:20 174:24	really 5:12 21:9 30:17 31:13 32:17,25 51:22 52:9,17 74:7 80:5 82:18 85:15 98:1 124:22 131:9 138:8 151:21 154:3 157:12 166:17 167:14 185:1 187:18 194:1 197:23 205:13 207:12 217:23 226:5,15 228:12,18 234:21 241:3 247:19 256:2	41:14 44:8 53:20 153:12 157:1 257:10 receiving 52:23 100:3 recent 232:4 recently 34:10 94:22 126:21 140:14 receptive 52:23 59:14 recess 124:13 206:9 rechargeable 194:22 recognition 23:14 recognize 23:3 125:1,6,8 recognizes 100:8 recommend 25:11 255:3 recommendation 205:23 recommended 24:4 162:17 reconcile 112:12 reconvene 206:1 record 5:13 6:11 7:7,14 22:10 23:7 24:10 25:9 31:9 39:17 43:15 53:24 64:25 65:2 116:10 118:7,24 122:6 123:24 138:12 143:11,20 155:25 178:1 204:7 208:12,24 214:9 215:8 226:11 231:2 232:23 244:21 262:8 recorded 208:4	recount 211:16 recounting 54:20 recoup 243:23 recouped 243:22 recovery 248:11 recreate 194:9,10 195:4 recycled 228:19 recycler 241:14 recyclers 238:16,21 239:4 246:5,22 247:1,10 256:15 recycling 209:20 241:5 red 6:23 reduced 262:7 reducing 116:9 reevaluated 74:1 refer 7:14 33:18 200:8 reference 92:21 199:23 referenced 93:3 references 121:22 referencing 149:8 195:7 referred 107:8 133:7 referring 7:6,10 refine 6:8 reflect 39:17 reflected 127:25 202:16 refrain 184:21 refund 167:23 refurbish 238:19 241:17 refuses 168:16
ranging 133:25 230:5 Rapid 7 8:21 rapidly 81:24 rare 35:23 rarely 148:23 149:1 155:3 rather 5:18 58:15 64:7 74:22 93:15 161:20 214:25 217:25 237:10 261:6 rational 28:18 reach 211:7 232:11 reached 55:3 153:10 156:23 react 22:7 53:16 92:11 reactivate 250:24 readers 186:9 reading 52:15 55:7 86:24 87:22 102:12 104:2,8 105:1,17,18 116:7,8,14 118:13 166:2 readings 118:12 119:19 ready 55:19 real 10:21 91:22 134:8 140:4 208:22 222:17 247:19 realistic 133:4 reality 43:5 127:19 131:11 175:21 realize 90:11	realm 75:4 84:9 real-world 73:24 reason 33:15 86:17 95:19 144:24 156:17 168:2 177:1 181:10 204:13 226:7 reasonable 58:2 65:21 98:24,25 99:17 104:25 172:4 178:13 189:22 reasoning 250:12 reasons 35:14 84:22 95:13,23 101:2 132:1 168:16 173:4 211:17,18 reassurance 57:5 rebuffed 77:14 recall 153:9 196:9 246:9 receive 18:16 20:15 41:5 201:23 238:23 244:2 246:6 257:6,8		

Regan 2:5 4:22 206:22	reinstate 260:20	207:17 208:4 209:7 238:10	replicated 200:24
Regan's 30:3	reinstated 224:16,17	remedial 195:18	replication 170:15
regard 133:18 134:15 152:8	reinstating 211:25	remediate 154:19 162:15 182:11	replies 41:5 44:13
regarding 38:2 98:17 100:4 129:6 198:11 213:10	reiterate 35:12	remediating 120:16	reply 40:12,23 60:1 121:24 157:1 211:19 242:19
regardless 223:21 245:18	reject 205:5	remediation 194:25	replying 44:14
regime 191:4	rejected 23:25 260:15	remediations 81:23	report 36:4 60:24 61:14 62:1,8 63:12 67:14 112:25 140:13 141:1 145:4 165:13 172:10,11 189:24 190:1 191:16
regimes 203:25	related 26:2 106:10 231:24 262:10	remedied 163:16	reported 1:16 96:19 156:4 178:7
regional 230:7	relation 6:10	remedies 195:14 197:23 228:9	reporter 6:13 156:23 208:5
register 16:8 23:25 232:3	relationship 58:6 77:15 78:8 150:9 200:7	remedy 56:11 125:16 214:3	reporting 1:17 53:6 57:25 58:1 59:4,9,10,15 64:14,15 66:19 67:4,13 69:20 204:14
Registration 262:23	relationships 134:24 241:13	reminders 247:12	reports 99:24 100:3 163:2 165:2,9 210:17
regularly 186:22 188:24 248:10	relative 262:13	remote 164:23,24	represent 7:21 157:15 209:18 229:22
regulations 152:17	relatively 20:1	remove 45:12 122:21 151:20	representation 18:4 19:21 20:16,20 209:10
regulators 98:12 99:7,8 179:6	release 174:6	removed 213:9 246:15	representative 70:8 149:13 246:19
regulatory 134:11 152:17 191:4	released 36:3 63:11	removes 213:20 239:7	representing 8:25 50:24 210:1 238:13 245:2 248:6
Reid 8:8,9,14 14:13,15 16:21 17:1,13 21:1,2 25:20 27:5,9 28:3,20 29:8,23 30:11,16,22 32:5,11 84:2 86:1,21 87:12 116:3,5 118:14,17,22 119:4 120:2,22 142:3 143:2 144:2,21 195:11,12 196:23 197:1,5 202:10 203:2,6 204:8,9	releases 46:13	removing 96:1	represents 157:12
Reid's 8:12 61:3	relentlessly 125:19	renew 217:18	
	relevant 95:12 152:20 231:10	renewed 232:7	
	reliable 75:11	renewing 217:19	
	relied 201:21	reopen 156:14 254:22	
	relieving 38:23	repair 12:12 162:19	
	reluctant 80:18	repaired 10:16 20:4,6 151:6	
	rely 37:12 38:16 42:16 47:12 99:11 105:22 125:21 177:7	repairing 12:12	
	relying 144:17	repairs 11:19 80:11	
	remainder 70:25	repeated 54:8	
	remains 215:17	replete 24:7	
	remarkably 61:25 73:13	replicate 175:2,7,10	
	remarks 9:18 90:9		

172:6 230:16 reproduce 186:11 reproducibility 187:12 reproducible 186:5 reproduction 148:20 reputational 97:21 130:23 request 35:12 51:17 88:8 92:16 147:12 199:24 requested 50:23 110:19 requesting 94:2 201:22 require 20:19 55:14 99:4 110:25 146:5 224:9 required 78:1 181:22 236:19 237:17 254:5 requirement 69:22 180:8 216:21 243:20 requirements 59:4 98:13 134:12 217:12 255:15 256:3 requires 65:10 103:4 128:19 147:17 175:8 requiring 220:9 research 3:3 10:1,25 11:11,25 14:19 16:4 20:9,18,21,23 21:20 25:13 27:7,19 31:19,22 33:15,17,21 34:1,7,15 35:11,18 36:6,8 37:7,15,18,20	38:6 39:1 41:9 43:7 45:7,11 46:2,22 47:1,2,15 48:1 57:12 62:3 68:1,8 71:3 76:11 79:25 85:5,7,10 89:7,14 90:1,3 95:21 96:13,15 97:17 99:10 104:11 107:6,12,19 108:22 109:12 111:2,5,22 112:5 113:2,5,13,16,21 114:8,9,21 115:5 122:1,2,11 124:15,24 125:9 126:3 127:8,14 129:6 130:13,14,21 132:6,18 134:22 135:3,8,13,23 138:18 139:4,23 140:9 141:13 142:6,7 149:21 152:1,10 153:25 160:4,6,18 161:3,14 163:6,9 171:5,14 173:14,16,18 175:7 177:9 180:11 181:7,20 184:18 190:16 192:3 193:19 194:19 200:13 203:17 researcher 10:7 38:9 39:12 54:6 56:24 57:6,8 58:1,3,25 59:2,11 60:5,14 61:16,17 64:13,16 67:5,11,16 72:2 78:4 85:7 87:17,21 89:15 99:20 103:20	104:18,21 105:22 106:13 107:9 108:3 111:10 128:4 131:3 139:17 140:21 141:23 154:24 156:25 187:23 188:1,2 189:7,13 191:24 194:10 199:6,14 200:2,14 201:1 202:13 researcher-centric 59:5 researchers 9:1 10:23 11:25 12:25 19:25 20:17 21:24 22:7 23:6,17 24:12,16 25:3 26:10 28:22 32:23 33:19 34:10 36:11 37:24 38:5,15,23 42:19 46:2 47:1,16 50:25 53:2,18 59:9 65:14,16,21 84:6 85:1 92:16 93:13 94:3 96:3 97:1 99:12,25 100:3,8 107:20 116:2 119:19 120:19 125:13 129:16 134:25 138:9 141:18 143:24 149:13 152:23 153:19 157:13 159:3 175:22 177:7 179:8 180:11,14,16 186:21,22 187:3,9 188:25 189:11,25 190:2 192:1,2,18 193:23 197:18 199:7 200:8 203:24 researcher's 59:13	67:2 125:15 researching 153:8 resell 238:20 241:18 247:2 resellers 246:23 reselling 222:13 reserve 70:24 resistance 11:23 resold 249:15 resolve 252:9 resolved 41:23 44:7,15 179:12 resolving 193:17 resources 12:14 66:3 69:9 76:14 189:20 193:14 respect 53:14 63:3 98:25 122:11 190:6 203:16 251:16,23 respecting 198:24 respective 41:20 respond 27:11 28:21 74:25 89:1 154:8 168:4 180:22 205:21 208:10 225:4 responder 75:16 responders 75:10 responding 6:1 226:14 response 17:12 63:7 91:2 94:23 100:22 141:16 143:7 173:9 176:21 177:10 235:11 responses 86:22 responsibilities 98:21 responsibility 98:19 256:10
--	--	--	---

responsible 31:21 79:24 91:17 99:21 130:25 134:22 135:8 142:8 152:22 178:5 responsibly 126:25 171:14,15 rest 60:22 121:19 restating 5:18 restoration 211:24 restraint 85:13 139:8 restrict 32:20 34:2 213:22 restricted 27:7 33:4 215:10,14 restrictions 214:20 216:18 259:23 result 20:2 50:12 61:19 73:20 74:3 79:6 82:11 222:23 227:19 230:9,17 resulting 211:24 results 13:1 20:4 31:22 63:23 97:18 140:5 163:10 resume 124:11 retail 249:15 retain 110:22 return 110:2 150:25 returning 146:19 153:4 returns 83:16 reveal 193:25 revealing 182:19 reverse 12:21	14:20 76:6 77:5 revert 260:11 review 93:1 207:25 reviewed 112:14 reviews 224:23 revoked 111:14 rewards 130:22 rid 143:18 194:21 ride 23:1 ridged 85:15 riding 141:3 Rightly 205:1 rights 213:16 rigidified 259:19 Riley 2:9 5:3 207:3 260:3,4 Ringer 4:21 risk 10:19,20,21,22 11:2 20:13 38:19,20 42:15 43:1 81:6 93:15,18 128:24 165:11 167:11 172:13 191:24 199:13 239:8 risked 44:2 risks 122:14 173:24 risky 76:18 138:3 188:6 road 6:12 66:8 85:22 roadblocks 96:1 97:6 roadmap 57:4 58:5 robust 97:17 107:19 role 72:23 100:9	134:13 190:5 room 1:9 23:5 94:12 153:19 173:11 180:14,17 root 51:11 rootkit 21:17 22:3 26:4 roughly 96:20 round 177:23 199:22 202:5 254:15 rounds 61:18 Roundtable 261:22 route 202:1 router 102:2 174:2 Rudimentary 50:2 rule 254:23 rulemaking 1:6 4:6 21:17 95:11 125:23 206:12 245:6 247:20 261:21 rules 6:12 160:10 run 93:23 101:20 111:20 115:10 205:10 running 71:7 76:10 102:1 103:24 109:12 113:15 114:5,15 115:15,16 runs 37:25 115:4 rural 230:6 Ruwe 2:8 5:1 198:7,8,13,17 207:1 <hr/> S <hr/> sad 125:18 SAE 135:2	safe 142:9 SafeDisc 22:3 26:1 safeguards 127:22 safer 23:10 safest 6:20 safety 44:3 46:4 51:14,15 62:18 134:1,4,9,14 135:16 140:7 150:18 152:13 154:5 179:25 saga 21:17 sake 6:14 sales 60:25 Samuelson- Glushko 8:15,18 35:4 sanctions 160:12 satisfied 235:8 237:18 244:6 satisfy 133:11 169:14 217:12 236:19 244:11 satisfying 122:16 save 210:22 saw 28:9 92:10 136:16 140:13 254:3 Sayler 8:17 34:18,19,25 36:20 37:5,6 174:12,13 176:17 195:10 198:2,4 scale 150:6 229:24 scanned 49:15 scary 197:9 scenario 13:17 82:17 103:8 108:2 120:5 168:14 218:22 219:11 220:16 222:15,17
--	---	--	--

225:14 226:10 236:18,19 237:14 240:10,14 249:13 251:7 259:14 scenarios 103:15 219:7 scenes 132:11 schedule 196:18 206:5 scholar 33:8 school 48:6 209:24 261:10 science 9:4,25 35:1 37:9 46:20 47:8 71:18 scientific 89:10 152:1 181:20,24 186:4,10 scientists 89:8 scope 106:7 110:6 111:11 113:17 215:20 247:21 249:10 scrap 209:20 238:15 screen 53:25 71:5 searching 107:23 125:19 second 53:9,12 75:5 91:15 97:8 116:18 142:15 151:7 174:1 180:6 193:13 204:21 212:6 218:16 235:20 236:6 240:13 245:25 248:25 secondary 67:1,7 76:2 256:23 Secondly 92:20 214:20 second-tier 61:17	secrecy 181:2 secret 83:10 89:21 90:2 secrets 132:18 133:10 148:10 section 4:5 12:19,24 14:17,18,19,25 15:16,17,18 18:9,11 20:12 21:20,22 23:13 24:14,25 37:13,17 38:4,10,24 51:3,20 70:6 71:8 86:25 87:14 99:2 113:2 119:14 120:4 122:8 139:22 145:10 146:5 178:17 206:13 213:7,12 223:21 232:6 239:6 245:14 sections 14:17 sector 32:22 33:18 secure 36:5 37:11 38:12 49:5,10 71:20,22 75:11 98:5,20 99:5 106:17 108:16 securing 53:3 security 9:1 10:2,7,9,20,23,2 5 11:1,8,11 12:25 14:12,18 15:3,7,8,10 16:3,4 20:10 21:20,23 22:6,7,15 23:5,14 24:2,11,12 25:3,13 26:10,12,22,24 31:18 32:23 33:19,20 34:1,7,10	35:1,11,24 36:7 37:6,14,18,20 38:5,9,15 39:1,2,3,11,13 40:25 42:19 45:6,11 46:2 47:1,2,16 49:2 50:25 53:18 54:6,7 55:1 56:24 57:5,12 58:24 60:5 62:3,12 63:11 69:14 71:2 72:2 73:8 74:1 79:3,24 84:1,6 87:18,21 90:20,25 91:5,20 92:1,9,15,24 94:24 95:21,25 96:2,15 97:11,15,17,20,2 5 98:12,17,21,24,2 5 99:6,8,9,10,13,1 7,21,25 100:5,7,8,9 101:1,4,23 103:12,14,20 104:11,18,21 105:21 106:13,23 107:19 108:3,4,21 110:6 111:5,17,22 114:15 119:19 120:19 122:1 124:15,19,25 126:3 127:7 128:9 129:6,9 130:24 131:3 132:6,18 134:14,22,24 135:3,8 136:8 138:14 139:4 140:21 141:13,18 144:17 147:7 148:13,14 149:14,21 151:5	152:1,10,22 157:13 158:6,9,12,13,15 20,23 159:2 164:10 170:24 172:2,5,15 173:19 175:22 177:7 178:13 179:7 180:1,24 185:24 189:17,18,21,22, 25 190:2 193:23 194:10,12 198:12,16 199:5,6,7,11,13 200:1,6,14 201:1 202:13 203:24 SecuROM 22:4 26:1,5 seeing 113:22 149:12 153:18 171:3 261:19 seek 101:11 105:25 106:4 107:5 111:1 113:18,19,20,21 246:6 seeking 56:17 106:4 107:15 109:14 118:4 127:15,20 214:3 231:23 258:20 seeks 248:11 seem 8:9 91:22 102:3 204:24 seemed 92:4 240:15 seems 55:9 59:17 110:14 221:19 239:20 252:24 seen 91:8 132:22 148:7 204:23 205:2 sees 159:17 224:3 select 257:1
---	--	--	--

selected 82:16	189:16 193:11	245:3	single 83:3 84:1
selective 81:7	server 102:1	shortcomings	sir 46:14 155:18
self-governance	106:22	14:24 22:1	site 91:18
187:4	servers 101:20	showing 152:15	sites 157:21
self-preservation	service 8:13	shown 37:15	sitting 25:3
93:24	189:13 219:20	showroom 259:14	197:9,10 208:22
sell 188:3 190:16	220:17 221:1,6	shrift 151:4	situation 33:25
192:4 223:17	223:25	shut 52:2 90:14	41:25 56:11 59:6
238:23 240:8	services 54:10	157:24	81:15 82:5,14
selling 188:17	97:10 101:8	sides 58:6	83:5,6 107:8
213:23	114:16 198:14	sideways 155:15	114:18 116:20
sells 117:13 247:3	231:6	sign 198:2 205:7	120:14 128:16
Senate 260:19	serving 230:6,8	signal 122:22	150:1 155:19
send 39:15,23 41:4	setting 60:9	184:4	217:9,13,15
57:6 122:22	settlement 251:2	signatures 123:4,5	218:15 222:10
217:22	252:7	signed 122:1,3	236:23,25 237:8
sending 40:13	several 4:17 11:3	224:8 246:16	251:16 257:11
90:22	12:16 14:16	signers 123:24	259:6
senior 5:6 9:7	15:23 26:2 35:7	significant 36:10	situations 111:21
178:4 189:16	74:12	38:18 58:13	157:23 179:7
207:6 209:14	severely 135:15	81:23 90:20	184:21 219:25
sense 65:7 79:23	severity 150:2	122:21 137:4	six 21:12 22:9
149:9 212:13,24	167:11	significantly 20:20	63:10 163:22
218:4 252:1	shake 61:6	56:11 215:10	Sixth 1:6 4:5
sent 55:22	share 8:11 55:5	229:24	206:12
sentinel 189:25	76:23 126:10	silence 23:19	skilled 147:23
separate 83:8	178:21 254:17	similar 19:1 33:25	skills 32:24
93:18 105:9	shared 53:19	56:16 73:14	skip 94:5 210:25
107:12 140:5	55:18,19 91:1,16	199:3 233:2	slide 54:20 55:20
184:15 186:12	128:20 171:1	similarly 196:20	56:12
separately 14:1	185:23 199:4	simple 12:23	slides 55:20
59:21	sharing 6:21	78:18 110:8	slightly 70:2 92:19
serious 11:5 13:7	178:19	simplest 78:19	120:3 236:12
21:9 23:15,22	sharper 112:11	83:2	slipping 25:22
25:8 38:11 47:13	Shaw 9:16	simply 13:7 14:7	sliver 190:19,22
54:17	shelf 240:3	18:11 23:9 31:9	Slover 209:14
85:12,14,20	Shellshock 36:14	80:25 152:16	210:14,16
121:9 125:25	she's 9:16 197:11	154:14 182:1	214:6,12,16
138:21 160:11	shield 161:25	189:5 225:23	215:15
194:14	short 21:3 124:13	simultaneously	216:7,10,13
seriously 91:21	151:3 155:20	163:4	218:18
178:3	206:9 213:18		219:10,13,19
served 113:3			220:13,17,23
			221:1,5 222:1,22

223:5,22 224:19 225:5 226:20 227:18 228:3 229:9,12 245:7 253:8,9 254:19 255:5 256:10 257:24 259:2,3,17 260:6,17 small 12:21 56:23 83:17,20 190:19,22 230:6 smart 45:22 48:21 102:9 140:22 Smith 2:5 4:22 25:16 26:17 27:6 28:2,11 42:5,7,14 43:22 53:23 55:2 56:1 57:13,23 58:8 76:20 77:18 78:12 79:18,21,23 80:2,21 81:13 109:21,24 110:1,4,10,16 111:3,23 112:3,13 117:5 132:16,22 133:2,11 198:18,19 199:25 201:2 203:3 206:22 Snapchat 99:16 Snort 39:21 so-called 90:8 social 201:19 society 139:24 199:11 software 9:13 12:22 14:9 22:19,24 23:23 31:11 34:9 36:12 37:11 38:18 77:5 101:8,16 102:1,25 115:9 117:8,10,12,15,1	6 120:22 121:11 124:15 125:15,20 128:3,9 131:15 132:8 134:6 135:9 136:11 145:5 147:4 152:3 153:20 154:2,11,18 155:12 173:19 176:23 179:2,9 180:9 183:8 194:24 195:2,23 196:22 197:4 212:18,19,21,22 213:2,6,11 245:19,24 261:1 Software-Security 3:3 sold 49:19 192:23 193:1 sole 54:25 125:15 232:10 solely 15:7 28:17 128:6 133:18 170:24 solicitation 53:5 solution 81:11 82:17 235:14 solutions 92:3 solve 121:14 solved 156:18,22 somebody 10:10,17 13:3 47:4 73:15 89:12 102:18 148:24 154:18 160:6,17,19 161:11 182:9 197:9 205:8 215:1 220:13 224:12 227:6 someday 15:21 118:25 somehow 204:5	240:17 someone 15:14 60:24 62:15 79:2 85:16 101:22 103:10,13 106:5,12,21 107:10 110:12 140:14 141:1,6 156:10 160:8 166:5 167:17,18 175:17 191:8 192:25 199:10 200:21 202:14 234:14 someone's 45:19 147:24 somewhat 6:22 37:22 149:8 190:9 somewhere 56:21 185:14 240:8 Sony 21:17 22:3 sophisticated 52:9,25 53:11 69:3 120:15 166:18 167:18 189:3 sophistication 53:14 170:8 sorry 4:3 13:9,24 20:3 27:10 36:16 56:13 58:17 89:5 90:6 131:9 147:22 155:14,24 160:24 161:13 169:6,22 181:11 214:4 216:12 218:6 242:15 249:21 259:12 sort 5:17,18,24 7:16 15:1 16:5 17:5 26:3,8 30:3,7,20 31:3 32:9 33:6 47:19 52:18 59:23 61:4 65:5 68:8 69:16	78:13,14 95:8 101:18 102:6,9,11 104:10 106:20,23 108:7,22 109:6,9 110:22 111:6 114:4,8 115:6,8,14,19,21 ,25 122:13 132:3,10,11 133:6,9 136:6 137:11,23 142:22,24 144:8 145:24 148:11 150:23 153:7,11,17,25 164:9 171:13 179:5,13 180:3,17 187:7 190:11 207:13,24,25 215:17,19 216:8 226:12 229:24 234:6 235:6 237:13 240:9,13,15,20 250:11,12,15 251:6 252:1,21 256:22,23 sought 18:23 76:22 144:1 sounds 77:18,20 140:25 255:11 source 48:13 148:9 space 24:19 180:1 spanned 10:5 speak 6:13 14:22 23:22 24:22 33:2 50:22 71:16 93:22 100:11 110:2 141:18 143:16 226:13 229:9 251:21 258:17 speaking 6:22
--	---	---	---

10:20,22 17:15 183:24 210:7 specific 7:10 37:19 42:7 80:8,9 125:13 128:15 130:3 132:17 136:6 137:17 155:21 156:13 167:24 168:1,25 171:25 172:20 173:9 174:4 177:3 180:1,4 183:21 185:10 205:18 232:23 specifically 26:18 72:22 121:23 125:22 132:23 139:11,15 156:16 161:8 246:4 250:5 specification 251:24 specifications 36:24 specifics 17:4 76:25 131:4 specified 245:20 specter 12:17 137:24 138:5 spectrum 184:12 185:20 speculative 24:4 129:3 speech 85:11 87:23 speed 134:3 spend 131:17 140:16 spent 12:13 46:21 spoke 18:20 94:8 132:3 spoken 98:2 sponsor 246:20	SSL 36:13 Stacy 2:11 5:5 207:5 staff 41:14 42:10 99:9 staffed 158:11 stage 247:20 Stahl 197:10 stakeholder 152:2 stakeholders 79:11,17 81:1 230:3 stall 163:21 Stallman 9:9 100:14,15,16 102:5,13 103:25 104:5,14,17,20,2 3 105:4,14,16 106:15,18,24 108:9,12,17,20 109:1,11,17,19,2 3,25 110:3,9,15,25 111:8 112:2,6,15,19 114:11,25 115:18,24 121:17,18 122:25 123:2,5,9,11,13, 18,25 180:21 181:14 stand 23:6 standard 29:17 64:7 65:9 66:13,23 68:6,11,15,21 69:1,4 72:13 77:7,8 84:18 86:10,18 88:12,13 119:7 128:23 129:23,24 133:6 189:22 199:21 standards 67:2 75:13 88:10	94:24 98:24 99:6 179:25 187:17 198:21 199:2,3,5,15,23, 25 200:4,8 201:6,7,12,15,18 ,22 202:7 Stanford 209:24 210:3 245:1 248:5 Stanislav 8:20 39:7,8,11,20 40:3,9,17,21 42:6,10,17 43:17,21,25 46:10,11,14 153:7,15 155:16 156:3 157:8,10 168:10 169:23 170:4 173:8,12 174:10,11,15 198:8,12,15 Stanislav's 117:7 start 7:21,24 16:1 34:20 51:5 85:15 107:21 177:18 197:6 208:20 209:2,6 211:20 214:8 261:15 starting 4:19 state 161:17,25 162:3,23,25 163:3 215:1 234:16 stated 171:7 192:20 199:18 246:21 247:5 260:6 statement 5:24 19:14 21:3 57:5 80:19 121:25 124:22 194:14 207:16 254:1 255:14 statements 7:23 182:24 208:16	254:12 statement's 19:17 state-of-the-art 158:6 states 1:5 99:3 stating 41:15 statistics 62:25 statute 28:16 37:21 103:4 202:19 statutes 122:12 203:18 statutory 22:2 69:22 95:13 127:12,21,25 137:12 stay 46:3 83:10 107:22 111:11,24 224:5 staying 106:6 steal 148:9 232:19 247:17 stealing 11:9 steering 134:3 stemming 24:2 stems 92:16 step 112:17 213:7 260:21 step-by-step 165:18 167:3 steps 166:24 185:10 Steve 2:8 5:1 62:7 123:20 207:1 Steven 8:22 46:19 stewards 114:19 stimulates 50:9 stolen 149:3 250:23 251:13 stop 13:20 184:5 248:11
--	--	---	---

<p>stopped 44:14</p> <p>stopping 253:4</p> <p>store 221:11,24 223:16 225:20 241:6</p> <p>Stored 122:10</p> <p>story 16:14 35:24 109:2 141:19 142:5,11 173:22</p> <p>straightforwardly 73:20</p> <p>streaming 43:12</p> <p>stretch 124:6</p> <p>strict 95:7</p> <p>strictures 57:9</p> <p>strikes 213:15</p> <p>strong 31:17 56:17 204:13 205:13</p> <p>strongly 84:19 126:13 152:13 230:20</p> <p>structure 29:16 85:15 110:24</p> <p>struggled 127:4</p> <p>struggling 66:7 101:14 167:14</p> <p>student 11:3 13:3 48:18 209:24 210:3 238:12 245:1</p> <p>students 18:14 19:25 20:14 23:9 25:4 32:16 33:9 47:20,22,25 48:24 49:6 72:3 75:7 160:21</p> <p>studied 48:13 51:1</p> <p>studying 34:25 38:15 48:14</p> <p>stuff 32:24 115:12 142:18 228:17 240:22</p>	<p>stumbled 72:7</p> <p>subject 47:15 166:10 178:7</p> <p>submissions 212:17</p> <p>submit 122:5</p> <p>submitted 7:8 208:1 245:13</p> <p>suboptimal 203:15</p> <p>suboptimally 203:17</p> <p>subscribers 230:7,10</p> <p>subsequent 27:14 46:13 54:20 55:21 59:6 61:15 236:18 237:17 244:4,10 251:6 253:14 254:6</p> <p>subsequently 60:18 63:11</p> <p>subservient 231:11</p> <p>subsidies 231:24 232:19 233:5 247:18 256:10</p> <p>subsidized 218:11,17 219:3,14,15 220:19 221:14,22 222:11 240:1,4,17 259:15</p> <p>subsidy 219:16,22 243:23 255:21</p> <p>substantial 21:23 22:10 100:20 239:8</p> <p>substantive 130:13</p> <p>substitute 214:18 215:11</p>	<p>succeeding 96:17</p> <p>successful 61:19 64:5</p> <p>successfully 248:17,19</p> <p>such-and-such 62:8</p> <p>suddenly 84:9</p> <p>sue 15:15 93:20</p> <p>sued 18:8</p> <p>suffer 96:24 97:21 248:12</p> <p>sufficiency 101:1</p> <p>sufficient 102:14 152:19 169:16 170:6 179:24 182:15 192:21 224:18 241:24</p> <p>sufficiently 76:4 107:19 172:15</p> <p>suggest 183:18</p> <p>suggested 68:23 88:11 95:10 244:9</p> <p>suggesting 51:25 82:15 88:6 114:3 115:23 190:13</p> <p>suggestion 63:20 88:9</p> <p>suggests 204:5</p> <p>summer 212:4</p> <p>superior 256:1</p> <p>supplement 148:21</p> <p>supplemental 86:3</p> <p>support 6:10 9:11 32:19 35:9 93:7 100:18 124:20 143:21 145:24 149:12 210:18 211:6 231:22,23 238:7</p>	<p>supports 126:13 230:20 247:15</p> <p>supposed 82:11</p> <p>suppress 11:25 37:17</p> <p>suppressing 38:2</p> <p>sure 13:11 14:15,21 17:24 19:13 27:5 29:8,23 30:11,16 32:5,11 33:21 35:14 37:1 43:21 46:10 55:9 70:24 82:23 108:25 109:23 113:13 139:1 143:2 151:11,24 154:10 157:14 164:13 165:8 182:20 183:14 186:2 205:20 216:7 222:17 233:1 234:13 236:22 240:24 250:14 251:11</p> <p>surrounded 124:22</p> <p>surrounding 234:2</p> <p>surveillance 72:20 75:17</p> <p>sweeping 161:9</p> <p>swiftly 181:7</p> <p>switch 225:18 226:17 228:16</p> <p>sworn 262:5</p> <p>Sy 2:6 4:24 206:24</p> <p>system 6:16,24 12:2,12,13 20:2,3,5 40:16 48:9,12 49:5,10 57:1 73:17 74:2 75:8,9,14 78:5 101:6 102:16,20 108:23 109:5</p>
--	--	---	---

111:19 115:4 116:25 117:7,16,18 120:7,17 128:5 131:20,21 138:7,19 140:17 146:24 147:6,24 148:3,15,24 156:5 161:10 164:11 165:19 168:2 169:1 171:1 172:5 184:23 194:5,13 202:8 204:1 systems 10:10,15 11:1,7,8 20:10 35:25 71:20,23 72:8,9,10,15,16, 19 75:12,16 82:12 106:14,17 107:3 114:2,5,6,13,22 115:4,11,15,17,2 1 126:23 135:9 139:5,13,24 140:3 141:11,24 143:19 144:5,6 150:18 161:4,5 199:12 <hr/> T <hr/> table 114:9,12 120:9 150:13 182:22 200:22,23 210:5 tablet 213:8,14 241:15 258:7 tablets 3:5 208:14 210:20 211:2,11 212:2,5 215:24 231:4 238:17 258:10 tailor 129:10 tailored 136:6 takedown 193:18 taking 55:10 56:9 121:8 250:9	254:12 talk 6:15 26:6 28:3 46:18 72:21 73:2 94:25 151:1 167:1 186:22 187:9 198:23 208:3 211:9 228:18 talked 197:21 256:21 talking 56:23 59:17,19 82:18 84:25 85:6,9,10,15 105:2 110:16 113:1 120:18 136:3 138:4 141:11 142:6 150:10 155:25 164:20 180:13,15 188:16 190:20 197:24 219:12 225:6,8 228:23 240:23 talks 60:1 tampering 144:10,11 150:18,23 tantamount 182:18 184:10 target 199:15 targeted 174:16 246:24 254:23 teach 48:24 49:6,7 159:23 team 54:15 55:19 63:12 67:12 91:2 teams 41:20 157:22 158:12 tech 8:18 69:3 technical 11:18 48:21 52:18 54:15 55:19 146:20 148:22	166:2 170:14 172:9 174:18 183:19 techniques 73:7,19 technological 13:23 26:13 134:7 145:6 147:16 148:11 technologies 159:25 technologist 193:12 technology 8:15 9:8,10 35:4 74:24 100:17 152:4 159:22 165:24 teenage 217:23 teenager 217:23 telecommunicatio ns 209:17 230:23 231:6 242:7 249:7 telephone 3:4 155:2 208:13 210:19 216:2 238:9 telephones 155:3 temperature 45:21 tempting 13:7 tend 52:1 tense 41:19 ten-year-old 189:9 term 229:16 terminate 234:17,23 termination 221:7 234:11,15,22 terms 7:6 64:10 99:8 130:4 138:10 141:13	152:12 172:20 233:13 254:17 terrible 182:25 terrifying 43:5 territory 77:3 Tesla 53:1 158:5,17 159:1 test 6:24 15:5 27:13 29:15 77:9 101:22 103:13 106:14,16,23 108:4,16 109:6 110:11 115:14 171:12 185:1,22 186:6,13 198:25 234:7 236:21 tested 105:19 115:8 161:10 testify 34:22 94:18 100:18 244:23 testimony 9:18 100:20 179:21 232:4 262:4,6,9 testing 14:12 15:3,7,10 16:4 18:17 26:23 37:20 87:18 101:1,4 104:4 110:6,8 111:17 114:4 115:12,21 124:19 128:7,8 139:4 147:6 tests 14:18 103:24 text 123:13,16 thank 9:20,21 12:10 16:11 20:24,25 21:2,6,10 34:19 37:4 39:5 40:19 42:23 43:25 46:6,8,17 50:14,15,20 61:22 71:12,15 88:25 94:15,16,17 100:10,13,15,17
--	---	---	---

121:15 123:18,25 124:1,12,17 133:15 135:17,18 137:19 141:21 142:1 146:6,8 147:1 149:4 152:5,25 153:1,6 154:7 173:6 174:9,11 178:22,23 180:19 181:13,16 186:16,19 187:19 198:1 202:9 204:10 205:24 209:13 238:6 243:13 244:23 248:2 256:17 260:2 261:8,11,18 thanking 34:20 thanks 25:14 71:16 94:15 154:6 163:13 198:17 220:1 237:24 that's 6:9 11:21 16:7 17:11,20 21:8 30:12,13,17,20 31:22,25 33:10 41:16 43:16 48:13 49:8 52:10 57:3,23 59:12 63:16,17 64:6,17 65:4 68:16 69:21,22 75:6,8 77:23,24 84:5 86:16 87:10 88:1,2,18 90:12,15 96:21 97:20,23 98:1,10 100:21 101:4 102:1 103:22 104:7,8 105:8,17 109:1,14 111:14,18,22	114:8,15 115:6,19,21,25 116:1 117:3,6,20 118:4 119:21 120:10 129:24 132:19 134:20 137:3,7,18 138:2,14 139:6,16 141:21 142:8,16,18 143:14,23 144:1 145:15 147:9,10,17,18 148:23 149:1 155:24 157:6 159:25 164:1 165:6 168:24 171:8 176:12,16 178:7,15 180:3 181:10,23 184:5,10 185:22,23 187:24 197:3 199:1 202:2,4 214:1 216:14 217:7,15,19 218:10 219:16 222:1,2,5,13,18 223:16 226:2,3,14 227:22 233:18 234:20 237:23 241:1,6,7,8,11,1 9 244:18 249:24 250:6,16 252:4,24 253:7,19 255:24 258:20 theft 125:25 243:3,4 250:6 251:4 theme 84:3 themes 10:18 themselves 165:10 themselves 4:18 70:19 93:16 96:16 103:23 105:6,11 122:10	137:17 185:5 199:8 206:19 225:10 theoretically 227:15 theory 31:13 thereafter 262:7 thereby 210:21 therefore 92:17 105:4 115:5 231:15 249:17 thereof 150:10 there's 14:11 20:12 29:6 34:15 52:7 53:4 62:9,18 68:4,14 80:20 84:18,23 86:21 87:5 88:7,14,23 89:11 91:19 92:22 103:16 106:1 113:25 119:4 122:17 130:14 132:12 136:25 138:11 143:20 145:3,5,7,8,10,1 6 151:7 152:9 154:20 158:7 159:22 165:14,15 171:11 176:14,18,22 182:24 183:9 184:8 186:20 187:2 188:12,14,15 194:12 195:2,22 198:23 204:13 206:3 207:24 215:11,19 217:8,12 221:6 223:1,18 226:5,12 229:17 253:2 the-shelf 115:9 they'd 218:25	they'll 24:21 they're 16:1,2,3,4,6 24:18 29:22 47:13,17,25 59:5 85:17 86:1 87:6,15 96:17 97:3 103:24 104:2,4 106:17 107:11,13,21,23 111:11 135:14 165:11 168:22 189:4 199:16 214:18 217:3 221:22,23 222:10 223:15,24 224:4 226:14,18 228:21,22,24 234:15,16 239:21 244:3 256:4 they've 28:8 98:17 129:2 179:10 180:1 191:20 213:14 217:3,4 224:5,8 225:11 248:21 third 55:3 98:9 106:12,22 109:5 Thirteen 63:3 thorough 65:20 thoughts 52:19 116:4 242:20 thousand 49:20 thousands 83:8 154:14 thread 157:2 threat 15:15 26:3 54:25 61:16,19 62:18 65:19 91:22 92:4 97:24 126:10 193:18 threaten 38:5 53:18 66:3 188:7 threatened 38:10
---	---	--	---

<p>55:25</p> <p>threatening 23:23 44:9</p> <p>threatens 65:17</p> <p>threats 22:8 23:8 38:13 51:2 53:20 71:2,4 126:1 190:5</p> <p>three-year-old 194:23</p> <p>thriving 129:4</p> <p>throughout 161:6</p> <p>throw 142:13 195:23 196:4</p> <p>thus 38:21 135:15 175:16</p> <p>thwarts 126:4</p> <p>ticket 156:12,14</p> <p>tie 202:11 207:10</p> <p>tied 32:9 242:23 257:16</p> <p>tier-one 157:17</p> <p>tip 7:1 208:9</p> <p>tire 194:4,13</p> <p>title 4:18</p> <p>today 4:7 5:11,16,23 7:12 8:3 10:12,24 14:16 20:7 21:11 22:12,17 23:6,24 24:16 25:1,4 26:7 27:16 28:5 34:23 35:3,15 44:17 48:14,19 50:22 51:11 71:17 72:3 86:18 94:25 100:11,18 119:10 129:16 133:22 160:14 198:23 205:19 207:12 210:7 211:9 222:10 223:21 230:12 238:7 244:24</p>	<p>261:13</p> <p>today's 9:19</p> <p>token 114:25</p> <p>tomorrow 261:14,16,19</p> <p>tools 14:2 76:7 78:1,5 89:12 126:23 127:1 187:2</p> <p>top 23:5</p> <p>topic 78:12</p> <p>topics 50:22</p> <p>totally 124:19 183:24</p> <p>toward 93:18 192:9</p> <p>towards 202:20</p> <p>toy 39:14,22 40:23 44:18 120:25 168:18,23 169:2,3 174:22</p> <p>toys 174:24 175:1</p> <p>Toys"R"Us 167:22 174:25</p> <p>TPM 12:23 13:24 14:7 31:10 117:6 150:3</p> <p>TPMs 21:22 22:4,5,16 24:2,23 35:10 74:3 134:8,13</p> <p>TracFone 211:4 222:9,14 225:4 227:24 228:8 229:14 231:24 232:10 233:19 239:11,24 240:22 242:19 243:19 247:12,14 248:9 249:12 250:10,17 251:18,21</p> <p>TracFone's</p>	<p>243:18 249:8 251:3 252:9</p> <p>tracing 253:24</p> <p>track 64:19 235:22</p> <p>tracking 45:17</p> <p>trade 76:7 98:13,22 99:3 132:18 133:9 148:9 193:12 238:13 241:11</p> <p>traded 175:20</p> <p>traditional 72:9</p> <p>traditionally 201:15,18</p> <p>traffic 14:5</p> <p>trafficked 181:1,8 249:14,17</p> <p>traffickers 232:19 246:25 247:17 248:11</p> <p>trafficking 14:1 77:25 78:8 225:6,7 226:10 239:14,16,17,21 240:22 248:1,8,12,14,18 249:3,9,13 252:3</p> <p>transaction 56:25 65:18</p> <p>TRANSCRIBER 263:1</p> <p>transcript 118:23 263:3</p> <p>transfer 227:10,13</p> <p>transit 114:2,6 115:4,17</p> <p>translate 167:10 168:7,8</p> <p>translating 172:9</p> <p>transmitting 40:7 43:13</p> <p>transparent</p>	<p>219:23,24 241:19</p> <p>treacherous 77:3</p> <p>treat 258:13 260:13</p> <p>treated 144:4</p> <p>Treatise 50:2</p> <p>tremendous 62:20 201:19</p> <p>trend 132:8</p> <p>triage 156:9</p> <p>tricky 205:16</p> <p>tried 31:17 146:25 168:12 233:1,9,18</p> <p>triennial 1:6 4:5 206:12 224:23 232:8 261:6</p> <p>triggers 200:25</p> <p>trivially 182:16</p> <p>Troncoso 9:12 110:1 124:16,17 130:1,10 131:8 132:7,20 133:1,5,13 135:19 136:2,22 137:5,18 153:3,4 178:24,25 179:17,20 202:12</p> <p>Troncoso's 166:12 175:13</p> <p>trouble 195:25</p> <p>troubles 72:4</p> <p>troublesome 144:23</p> <p>troubling 87:25 88:5 149:19</p> <p>true 165:6 248:16 262:8</p> <p>truly 124:5 240:15</p> <p>trust 81:18</p>
---	--	---	--

125:6,7 172:9,14 trusted 190:1 truthfully 50:8 try 6:14 7:2,5 21:3 49:8 67:22 68:2,13 93:19 162:11,12 184:8 206:4 208:3 229:25 236:9 252:9 trying 17:20 23:10 59:22 66:7 67:25 78:15 90:3 92:8 103:7,15 104:14 106:22 109:9 113:16 117:24 118:2,20 121:14 130:22 142:21 143:11 145:19 146:2 148:19 166:11 188:8 190:14 196:23 222:6,18 236:25 249:14 252:6,23 253:4 Tuesday 1:7 turn 6:21 124:16 149:19 150:15 184:4 214:25 238:11 256:2 turnout 205:13 TVs 45:22 Twenty 48:2 twice 90:18 211:21 Two-factor 198:15 twofold 204:15 two-part 240:14 two-way 75:9,12,15 two-year 221:2 233:6,15 234:10 type 51:11 52:23 53:9 55:14 84:13	114:15 127:13 131:19 136:11 149:22,25 182:3 183:3 190:1 191:1 197:5 199:5 200:22 241:20 types 52:22 73:8 103:18 136:7 139:23 typewriting 262:7 typical 62:23 167:25 typically 131:1 typing 197:7 <hr/> <div style="text-align: center;">U</div> <hr/> U.S 2:2,4,5,7,8,10,11 4:9,21 37:8 72:12 188:22 192:22,24 193:2 207:6 U.S.C 121:23 ubiquitous 35:19 107:3 Uh-huh 109:25 ultimately 17:19 41:13 45:18 58:14 153:12 245:16 246:15 unauthorized 41:1 132:19 139:13 unaware 45:13 uncertain 122:11 uncertainty 113:23 119:12 122:14 247:10 unchanged 91:11 123:14 unclear 102:14 103:3 207:20 235:4 uncomfortable	33:3 131:25 141:5 underestimated 22:14 undergraduate 48:23 underlying 85:18 137:12 245:19 underpins 22:24 underscore 30:23 85:9 195:13 197:22 underscored 22:10 84:16 underscores 23:14 100:24 understand 6:16 16:19 30:2,4 40:4 44:10 48:8 52:8 59:23 66:24 99:25 109:9 111:15 113:6 157:22 162:22 166:6 178:16 185:12 191:2 204:18 215:19 222:19 226:8 228:25 235:3 243:17 understanding 13:15,19 14:6 54:16 55:17 136:21 165:24 185:11 186:3 195:15,16 229:8 understood 42:14 54:11 239:25 undertake 10:24 175:11 188:5 undesirable 113:4 undue 37:23 38:23 unexpectedly 81:23 unfair 98:13	unfortunate 42:25 122:13 175:20 unfortunately 24:6 35:23 37:13 53:10,18 129:4 158:8 175:21 203:15 unhappy 74:10 141:25 unhear 118:14 unintended 82:5,9 126:5,18 128:16 unintentionally 45:15 Union 209:11,15 210:17 228:3 257:23 260:5 unique 36:9 174:22 UNITED 1:5 units 133:24 universal 231:21 universe 23:23 university 8:16,19,23,25 9:5 10:12 11:24 19:24 33:7,15,25 35:2 46:20 71:19 159:12,14,17,19 160:16 209:10 unknown 181:3,6 unlawful 243:2 251:25 252:2,11 255:17,19 unless 94:5 146:24 182:21,23 233:12 unlimited 50:10 unlock 165:4,5 210:19 214:22 216:19 217:5 225:18,25 228:20 230:21 231:10,15,19
--	--	--	---

<p>233:11 234:1,25 239:5 244:2 246:4,6</p> <p>unlocked 223:10,17 233:17 236:7 249:9 257:15</p> <p>unlocker 253:23</p> <p>unlockers 246:13</p> <p>unlocking 3:4 28:10 164:23,24 206:6 208:13 212:7,12,14 213:9 214:10 215:2 228:7 231:18 232:25 238:8 239:12 245:4,6,8,11,16, 17,22 246:1,2,3,8,11,1 2,16,22 247:6,7,8,13,15, 21 249:4 252:15 253:5 258:7 260:9 261:12</p> <p>unmindful 49:20</p> <p>unnamed 192:22</p> <p>unnecessarily 186:13</p> <p>unnecessary 213:20 245:16 248:14</p> <p>unquote 246:23</p> <p>unreasonable 38:20</p> <p>unsafe 80:17</p> <p>unscrupulous 23:18</p> <p>unspecified 192:23</p> <p>unsubsidized 219:8</p> <p>unsuccessful 64:4 65:2</p>	<p>untouched 76:12</p> <p>unusual 48:8</p> <p>unverifiable 24:3</p> <p>unwanted 238:18</p> <p>unwilling 179:9</p> <p>updated 123:1 155:3</p> <p>upfront 15:2</p> <p>upgrade 217:25</p> <p>upon 41:9 72:7 125:14 131:21 186:7 187:11</p> <p>uproar 211:22</p> <p>urge 129:9 144:3 179:11</p> <p>urged 21:18 22:6 23:3 224:23</p> <p>urgent 91:8</p> <p>usability 75:20</p> <p>usable 67:15</p> <p>useful 200:15 210:22 213:18</p> <p>user 125:6</p> <p>users 83:12,18 120:15 152:3 154:24 161:20 162:15,18 176:22 232:14</p> <p>usually 218:7</p> <hr/> <p style="text-align: center;">V</p> <hr/> <p>vague 193:24,25</p> <p>valid 241:20</p> <p>valuable 180:12 183:4 189:19</p> <p>value 74:17 140:9 181:1,8 192:24 201:20 228:19 238:23</p> <p>variation 111:16 158:8</p>	<p>variety 22:25 75:14 79:14 201:16 238:24 248:10</p> <p>various 54:10 72:18 134:24 135:1,5</p> <p>vary 184:11 185:19</p> <p>vast 22:19,20 34:7 142:5</p> <p>vector 190:4</p> <p>vehicle 33:20 134:5,10,11,14</p> <p>vehicles 35:21 36:15 133:22 144:10</p> <p>vein 146:11</p> <p>vendor 41:10,12,15 44:5,13 45:1 63:14 79:7 89:18,22,23 93:19,20,25 131:2 151:23 156:24 159:10 163:21 173:23 174:6 180:9</p> <p>vendors 91:24 93:14 97:19,20,25 98:14,16,18 99:4,7,13 157:11,12 161:16,18,22 162:2,9,13,18 163:4,6,8 188:7 190:5 204:22 205:1</p> <p>vendor's 41:21</p> <p>venue 47:8</p> <p>venues 145:13,22,25</p> <p>verify 58:25 186:11</p>	<p>version 136:25 229:7</p> <p>versions 239:20</p> <p>versus 16:20 47:1 82:19 172:21 229:14 260:25</p> <p>via 37:8 39:25 176:20 230:25 233:7</p> <p>victim 203:24</p> <p>video 22:19 25:17,18,24 26:1,14,18,21 27:7,15,18,23 43:12 52:12,13 197:9</p> <p>view 13:8 16:24 19:9 50:10 83:1 100:20 185:23 186:1 236:4,24 237:6,7,9 239:22 241:25 251:2 252:13</p> <p>viewed 139:14</p> <p>views 23:7</p> <p>vigorous 126:7</p> <p>VIN 196:16</p> <p>violate 146:16,17 148:2,25 204:5</p> <p>violates 122:12</p> <p>violating 18:11 24:25 160:12</p> <p>violation 20:12 34:13 87:5 99:2 120:8 121:22 128:12 133:8 148:4,20 191:21 203:4</p> <p>violations 45:7</p> <p>virtually 72:24 136:11 226:24</p> <p>vis-a-vis 220:22</p> <p>viscerally 53:17</p>
---	---	--	--

visibility 180:23 visible 66:18 67:3,15 132:13 vital 133:25 134:13 247:8 voice 150:17 160:25 voicemail 40:16 115:3 151:14 voluntarily 178:12 voluntary 214:13,14,17 215:5 voting 72:14,16 161:4,18,20 162:2,9 VPN 102:17,18,21 103:8,10 105:23 vulnerabilities 10:9,21 11:5 12:1 22:15,18 24:2,11,24 25:25 27:14 36:10,14 41:18 43:10 44:24 46:12 47:13,23 50:4 54:15 55:11 72:7 96:1,3,6,8,13,16 97:2,8 100:4 120:21 125:14,19,24 126:24 129:1,7 130:24 131:16 135:14,23 136:8,18 137:16 140:6,11 151:6,18 152:24 153:22 154:3 159:9 161:4,9 173:5 180:2,8 187:22 189:2,3,4 191:4 192:18 193:1 194:4 197:2 vulnerability 13:8 34:11 36:4,9	47:4 53:11 55:1 58:2,7,22 59:14 60:3,23 61:10,18 62:1,25 63:3 64:15 69:15 74:12 80:8,14,24 82:10 83:7,23 84:1 91:1 92:24 97:22 98:3,7,9,11 99:22 102:19 105:5 107:11,15 126:11,20 128:14,19 131:5,11,12,19 153:8,14,16 154:13 155:5 156:20 163:16,19,22,23, 25 164:17,21,23 165:3,12 166:3,14 167:4,8,11 168:8 170:15 171:23,24,25 172:3,21 174:5 175:3 180:7 181:7 182:5,12 183:9 184:3,7,9 185:2 187:21 188:2,4 189:9 190:25 191:9,15 192:21 193:2 194:12,20 195:16,17 196:12,22 200:6,13 204:14 vulnerable 22:23 108:23 155:8 182:11 184:2 196:13 199:12 <hr/> <p style="text-align: center;">W</p> <hr/> wait 142:15 196:2 waiting 96:12 waived 237:20 walk 221:11,24 222:19,20	223:7,16 225:24 233:14 259:14 Walt 10:8 warn 74:18 80:15 166:20 warned 21:21 warning 151:8 warranted 129:9 211:18 wash 188:4 Washington 1:10 4:11 91:4 wasn't 17:15 42:12 55:8 84:23,24 88:3 91:23 162:2 218:16,19 waste 213:20 watch 124:9 watching 45:17 ways 10:19 12:12 29:16 49:7,11 70:20 75:22 128:16 139:13 143:5 211:13 223:1 weaknesses 72:18 75:19 web 36:5 43:8,16 45:1 49:16 66:20 173:15 196:17 website 54:12 66:18 83:17,20 108:5 109:5 256:25 websites 53:6 83:8,17 132:14 154:14 158:14 we'd 76:16 78:9 84:24 86:2 119:22 131:24 254:12,21 255:10	week 4:12,14 35:23 36:1,17 80:24 weeks 34:14 38:9 82:10 194:9 week's 36:9 weigh 93:15 95:9 224:2 weird 115:2 Weissenberg 209:23,24 243:15 244:20,22,25 256:7,8 258:17,19,23 welcome 4:5 40:21 52:24 206:10,11 we'll 7:21,22,24 8:12 22:17 34:17,18 70:23 86:5,8 94:11 118:17 123:16 124:10 173:10 177:23 206:6 208:20 209:1,5,6 240:25 well-defined 78:21 well-known 47:5,12,23 we're 5:8,21 6:6 7:3 15:24 17:20 26:6 27:19 29:24 30:2,19 31:15 32:1,15 48:3 51:10,17 53:24 56:23 66:7,13 68:16 70:2 78:22 79:1 82:8 85:5,9,10 86:7 88:18 90:2,11 94:2,5 113:15 116:21 117:15,17,18,24 118:2,19,24 119:2 121:14 124:14 136:9
---	---	---	--

141:11,25 142:6,21 143:8,10,11 144:22,24 145:19,24 146:2,12 150:10 152:12 153:18 155:25 170:18 171:10 175:24,25 176:5 179:3 180:13,14 181:22 185:14 190:14,20 195:8 197:24 204:9 211:7 221:16 222:6,22,23 223:5 225:6,7 228:23 233:7 235:19 236:3,24 241:8,12 242:3 248:5 258:16,19 261:13 we've 5:20 7:12 15:22 22:13 31:8,16 37:19 58:4 66:22 70:20 78:10 88:9 129:21 137:23 197:16 205:10 210:24 219:14 239:10 255:25 whatever 66:14 85:4 101:21 116:25 147:20 154:9 157:24 168:16 177:8 227:24 257:19 whatevers 46:23 whatsoever 110:19 134:18 Whereas 47:10 Whereupon 54:2 123:21 124:13 206:9 261:20 wherever 234:25 whether 15:2,6,9 20:12 27:6 29:12	32:8 37:25 50:3 56:2,3 58:9 59:13 60:6,20 64:13 67:3 86:8 87:5,6,17,19 88:16 89:20,22 98:13,15,16 103:3 106:17 111:3 122:11 140:3,4 143:23 144:5 150:3 159:9 162:8 165:10 167:22 169:2 171:13,14 172:13,14 174:2,7 182:17 184:6 185:1 213:10 217:1 219:6,7 228:19 231:16 235:7 237:18,19 244:6 245:18 250:23 251:13 255:16 258:9 261:5 white 6:23 101:22 whoever 102:22 whole 50:5 91:21 92:2 107:23 144:12 176:25 185:19 186:20 201:16 wholly 107:12 whom 81:8 106:4 169:15 262:2 whomever 40:13 who's 33:24 81:12 167:17 168:7 178:5 192:17 193:1 202:14 217:20 whose 107:5 110:13 262:4 who've 62:7 wide 22:25 23:23 174:24 widely 114:22	135:14 185:23 189:9 widen 46:1 wider 116:14 widespread 22:14 wife 237:4 wild 91:15 92:1 willing 117:13 141:9 143:18 165:11 172:13,14 179:22 229:6 win 44:19,21 window 128:25 Windows 101:21 winds 30:24 wire 195:8 Wired 54:8 wireless 3:4 11:7 194:4,13 208:13 210:21 212:10 216:2 217:11 230:3,5,10,11,14 ,15,22 231:4,17 232:15 238:8 239:2 242:7 249:6 250:21 257:17 260:10 Wiretap 122:9 wiretappings 72:19 wish 93:1 withheld 90:19 witness 262:4,6,9 won 48:16 248:21 wonder 56:1 216:6 wondering 27:4 55:7 76:21 78:13 114:7 124:4 133:2 141:8 wording 247:21 work 12:15,20	13:25 14:9 17:8 23:20 28:4 32:16,18 37:25 71:21 72:2,5,23,25 74:5,17 75:5 76:16 78:10 79:4,6 80:20 89:9,21 94:21,23 99:12 117:19 132:11 138:2 142:8 153:13 157:12 175:10 181:22,23 186:11 194:9,10 202:22 214:21 220:21 238:21 242:11,13 261:17 workable 24:13 25:18 111:5 workaround 163:1 Workbench 49:3,25 worked 6:5 10:7 27:25 33:22,23 42:18 48:9 71:25 198:10 232:9 working 4:4 33:9 52:10 78:6 94:20 124:23 141:24 184:5 226:20 260:18 workings 65:11 works 20:22 81:1 111:16 145:1 165:24 199:12 world 39:4 40:3 101:7 171:4 175:21 176:1 222:18 worried 125:12 143:5 145:15 worry 194:23,24 208:7 236:8
--	--	---	--

237:1	168:13 179:4		
Worse 41:3	184:7 207:25		
worsening 24:1	216:21 218:2		
worst 20:22	219:1 220:24		
worth 42:25	226:21 250:9		
195:24	252:14,16		
wow 50:19	257:3,10		
wrap 70:23 261:13	<hr/>		
write 83:4 166:10	<u>Z</u>		
168:11 171:17	zero 175:15 176:6		
186:10 229:4	188:21,23		
writes 174:15	zero-day 125:22		
writing 183:13	129:6 179:14		
208:1 254:9	180:6 187:21		
written 5:19 7:8	190:19,25		
76:17 150:12	191:4,9		
177:3			
187:6,14,15			
198:21 207:24			
211:10 212:16			
254:12 255:21			
wrong 13:21			
218:22 240:18			
wrongly 205:1			
wrote 48:10			
<hr/>			
<u>Y</u>			
Yahoo 82:12			
83:13			
Yep 234:19			
yet 53:10 158:11			
175:16 260:8			
yield 245:10			
you'll 22:11 27:16			
176:15			
young 11:12			
yourself 7:18,19			
33:8 62:14			
217:25			
yourselves 144:15			
you've 5:19 59:21			
85:11 119:10			