

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner.

IPR2024-00332
U.S. Patent No. 10,929,512

IPR2024-00334
U.S. Patent No. 11,514,138

REMOTE DEPOSITION OF MICHAEL T. GOODRICH, Ph.D.

(Taken by Petitioner)

January 8, 2025

12:02 p.m.

Deposition held via Zoom Videoconference

Reported by: F. Renee Finkley, RPR, RMR, CRR, CLR,
CCR-B-2289 (Via Videoconference)

Henderson Legal Services

202-220-4158

www.hendersonlegalservices.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

APPEARANCES OF COUNSEL

On behalf of the Petitioner:

HONG SHI, Esq. (Via Videoconference)
DAVID W. O'BRIEN, Esq. (Via Videoconference)
KELLY LYLE, Esq. (Via Videoconference)
Haynes and Boone, LLP
98 San Jacinto Boulevard
Suite 1500
Austin, Texas 78701
(512) 867-8440
hong.shi@haynesboone.com
david.obrien@haynesboone.com

On behalf of the Patent Owner:

GEORGE FISHBACK, Esq. (Via Videoconference)
McKool Smith, PC
303 Colorado Street, Suite 2100
Austin, Texas 78701
(512) 692-8700
gfishback@mckoolsmith.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CONTENTS	
THE WITNESS: MICHAEL T. GOODRICH, Ph.D.	
EXAMINATION	Page
By Ms. Shi	4
EXHIBITS	
Exhibit No.	Page
1 - Table of contents to Introduction to Computer Security	16

1 (The witness was sworn.)

2 MICHAEL T. GOODRICH, Ph.D.,
3 having been first duly sworn, was examined and
4 testified as follows:

5 EXAMINATION

6 BY MS. SHI:

7 Q. Good morning. Again, I'm Hong Shi from
8 Haynes and Boone on behalf of Petitioner Apple.

9 A. **Good morning.**

10 Q. Good morning. So I will go over some of
11 the ground rules, similar to what we did yesterday,
12 but this is specific for this deposition. So do you
13 understand that you're under oath today?

14 A. **Yes.**

15 Q. And you understand that the oath requires
16 you to answer my questions truthfully and completely?

17 A. **Yes.**

18 Q. And you will answer truthfully and
19 completely today; is that right?

20 A. **That is my plan.**

21 Q. Is there any reason that you cannot
22 provide truthful, complete, and accurate testimony
23 today?

24 A. **No.**

25 Q. Is there any other reason that your

1 deposition should not go forward today, medical or
2 otherwise?

3 **A. I don't anticipate any problems. We're**
4 **having wild fires here in Southern California, but I**
5 **don't think any of them are near to here.**

6 Q. Good to know. But if there's an emergency
7 of the wild fire, let me know. We don't want you to
8 be in danger just for this deposition.

9 **A. Thank you.**

10 Q. I would like to ask you to focus on the
11 questions I asked, and answer that question, not
12 another question; is that fair?

13 **A. I will do my best.**

14 Q. And we can plan the breaks as we go, but
15 let me know if you need a break any time.

16 **A. Okay. Thank you.**

17 Q. So today, we're here discussing the cases
18 for the '512 IPR and the '138 IPR; is that clear?

19 **A. That is my understanding, yes.**

20 Q. So for this set of questions, it applies
21 to both declarations. I won't -- if it goes into the
22 specific of any separate declaration, just let me
23 know, but this set of questions should apply to both;
24 is that clear?

25 **A. Sure.**

1 Q. So for preparing for those declarations,
2 did you review any documents?

3 A. Yes.

4 Q. What are they?

5 A. I speak to this in my declarations. I
6 list, for example, in my declaration for IPR for U.S.
7 Patent 10,925 -- or 929,512, which we call the '512
8 patent. I list those in my paragraph 15.

9 Q. In addition to those documents listed
10 there, did you review any other documents for
11 preparing your declarations?

12 A. I also recall reviewing a declaration from
13 Dr. McDaniel in each IPR. I also reviewed the
14 decision from the board to institute IPR in each
15 case. There may have been some other documents as
16 well I'm just not recalling, as I sit here today.

17 Q. To prepare your declarations, did you
18 review the Patent Owner's preliminary responses?

19 A. I don't recall, as I sit here today.

20 Q. Did you review the petitions in their
21 totality?

22 A. I reviewed them. I don't recall if it was
23 the entire documents in each case. In some cases,
24 there oftentimes are legal arguments in these
25 proceedings. And I tried to stick to the technical

1 **arguments.**

2 Q. Did you meet with anyone to prepare for
3 your declaration, either remotely, or by e-mail, or
4 in person?

5 A. Yes, I met remotely with Mr. Kamprath from
6 McKool Smith, Mr. Jarrett at McKool Smith, and
7 Mr. Fishback at McKool Smith, who I believe are
8 representing the Patent Owner.

9 Q. Did you talk to anyone else?

10 A. I don't recall talking to anyone else, as
11 I sit here today.

12 Q. Did you do anything else to prepare for
13 the declarations?

14 A. I also studied the patents. I did my
15 typical methodology of looking at the arguments,
16 thinking about them, placing myself into the shoes of
17 a person of ordinary skill in the art, in light of
18 the alleged prior art. And then in discussions with
19 counsel, I came to my conclusions.

20 Q. Do you remember roughly how many hours you
21 spent to prepare the two declarations?

22 A. No, I don't recall that.

23 Q. Do you have a rough estimate?

24 A. I am not comfortable speculating. I don't
25 recall it.

1 Q. So to prepare for the deposition today,
2 have you reviewed any documents?

3 A. Yes.

4 Q. What documents did you review?

5 A. My recollection is that I reviewed my two
6 declarations. I reviewed the declaration -- at least
7 one of the declarations from Dr. McDaniel. I
8 reviewed the institution decision. I reviewed some
9 of the prior art references.

10 Q. Did you review the Patent Owner responses?

11 A. Not that I recall.

12 Q. Did you review any draft of the Patent
13 Owner responses?

14 A. Not that I recall, just sitting here
15 today.

16 Q. Did you meet with anyone remotely, in
17 person, or through e-mail to prepare for your
18 deposition?

19 A. Yes, I met remotely with Mr. Jarrett and
20 Mr. Fishback.

21 Q. When was that?

22 A. That was on Monday of this week. This was
23 joint with the other depositions that we had
24 yesterday as well.

25 Q. And how long was that?

1 **A. It was a few hours.**

2 Q. And did you review the documents you
3 mentioned after your meeting with your counsel?

4 **A. That's my recollection, yes.**

5 Q. When was the last time you reviewed the
6 documents to prepare for today's deposition?

7 **A. I did some review yesterday after our
8 deposition from yesterday.**

9 Q. Did you also do some review today before
10 the deposition?

11 **A. No.**

12 Q. Did you review any documents filed or
13 prepared for the District Court?

14 **A. Not that I recall. Only if there's
15 potential overlap, for example, with any of the
16 alleged prior art references, for example.**

17 Q. But you're not aware there are any
18 documents specific for District Court litigation?

19 **A. That is correct.**

20 Q. Let's -- again, do you have the
21 declarations on your computer?

22 **A. I do. In anticipation of how we did
23 things yesterday, I have them on my screen.**

24 Q. Do you have notes on them?

25 **A. There's no notes. There's only some**

1 **sections that may be highlighted in yellow.**

2 Q. So let's go to the -- your declaration,
3 Exhibit 2037, for the '512 IPR?

4 A. **I am there.**

5 Q. Can you go to the last page of your
6 declaration?

7 A. **Yes, I'm there.**

8 Q. Is that your signature on the last page of
9 your declaration?

10 A. **Yes.**

11 Q. Did you sign after reviewing the entirety
12 of the declaration?

13 A. **Yes.**

14 Q. Is there any error in your declaration
15 that you would like to correct?

16 A. **I noticed in reviewing, that there's some
17 minor typos, but they are not, in my opinion,
18 substantive. There's nothing substantive that I wish
19 to change at this time.**

20 Q. Let's go to paragraph 8 of your
21 declaration.

22 A. **I am there.**

23 Q. Can you read the first sentence of
24 paragraph 8?

25 A. **"I have taught undergraduate and graduate**

1 **courses concerning algorithms, data structures,**
2 **software design, networking, and computer security,**
3 **beginning with my work as a graduate student at**
4 **Purdue in 1983, and continuing as a professor at**
5 **Johns Hopkins and University of California, Irvine."**

6 Q. Can you describe the courses you taught
7 concerning algorithms?

8 A. Sure. So I believe this was also in my
9 CV. I will pull that up as well. Yes, the courses
10 that I have taught that include discussions and
11 lectures on algorithms include computer security
12 algorithms, computational geometry, computer
13 graphics, cyber fraud detection and prevention, data
14 structures, graph algorithms, fundamentals of
15 algorithms with applications, introduction to
16 algorithms, Internet algorithms, design and analysis
17 of algorithms, parallel algorithms, project in
18 algorithms and data structures, text processing, and
19 pattern matching.

20 Q. So for the courses you have here, what are
21 the courses that concerns networking?

22 A. So courses that include networking are
23 advanced parallel computing, computer security
24 algorithms, cyber fraud detection and prevention,
25 graph algorithms, Internet algorithms, parallel

1 **algorithms, project in algorithms and data**

2 **structures, text processing, and pattern matching.**

3 Q. And what are the courses you have taught
4 concerning computer security?

5 A. So courses I've taught that include topics
6 of computer security, in addition to the textbook
7 that I coauthored, include computer security
8 algorithms, cyber fraud detection and prevention,
9 Internet algorithmics, text processing, and pattern
10 matching.

11 Q. And you have been teaching these classes
12 since 1983; is that right?

13 A. I've taught courses that -- these were
14 part of the whole suite of courses, so they began in
15 1983, my teaching.

16 Q. So for the networking classes, when do you
17 remember you first taught the networking classes?

18 A. Courses that included networking, my
19 recollection is they began in the early 1990s.

20 Q. And do you remember, when do you first
21 start to teach the computer security classes?

22 A. My recollection is I started teaching
23 those classes in the late 1990s, early 2000s.

24 Q. So you have one course called computer
25 security algorithms; is that right?

1 **A. That's right.**

2 **Q. Is it open to -- what level of students**
3 **are they directed at?**

4 **A. I taught computer security algorithms, as**
5 **I recall, to early undergraduates. So the goal was**
6 **to design it for freshmen and sophomores, but there**
7 **may have been some upper classmen as well.**

8 **Q. And the computer security algorithms**
9 **classes, do they sometimes just be referred to as**
10 **computer security classes, or is it limited to**
11 **algorithms?**

12 **A. I think people may have also referred to**
13 **that as a computer security course.**

14 **Q. What specific topics do you cover in your**
15 **computer security class?**

16 **A. So as I mentioned earlier, I coauthored a**
17 **textbook called Introduction to Computer Security.**
18 **And so as a part of this course on computer security**
19 **algorithms, I -- it's not surprising, since I wrote**
20 **the book, I went through the chapters of my textbook.**

21 **And more advanced topics, I tried to**
22 **explain them to the students, so they could**
23 **understand, 'cause like I said, I was going for**
24 **undergraduates for that class. And so the topics**
25 **that I discussed roughly coincide to the chapters in**

1 my textbook called Introduction to Computer Security
2 coauthored with Roberto Tamassia, T-A-M-A-S-S-I-A.

3 And the topics included access control,
4 cryptographic concepts, implementation and usability
5 issues, physical security, operating system security,
6 malware, network security at the lower layers of the
7 network stack, network security at the higher layers
8 of the network stack, including applications, web
9 security, cryptography, including encryption and
10 decryption, security models and practice, and
11 application security.

12 Q. Is it correct that you keep the computer
13 security course up to date with the latest
14 developments in computer security?

15 A. I'm not quite following your question.
16 I'm sorry.

17 Q. Do you make changes every year to your
18 course materials to reflect new trends in computer
19 security?

20 A. I don't recall the last time I taught this
21 class exactly. It's been several years since I've
22 taught it. Other people now are teaching that class.
23 And I presume that they're teaching more recent
24 topics, but I don't know that in detail.

25 Q. Did you cover social engineering in your

1 computer security class?

2 **A. I believe so, because this is one of the**
3 **topics that is in chapter 1 of my textbook.**

4 Q. Are you reading the topics from your book?

5 **A. Yes.**

6 Q. Do you have -- I would like to ask you
7 without -- don't consult external materials without
8 disclosing it, would that work?

9 **A. Yes, so I'd like to disclose that I am**
10 **reading from my textbook to refresh my recollection**
11 **about the topics that I taught, since I taught from**
12 **my textbook. And the title, again, is Introduction**
13 **to Computer Security by Michael T. Goodrich and**
14 **Roberto Tamassia, published by Pearson with a 2011**
15 **copyright. I believe this is available on Amazon, if**
16 **you'd like to purchase a copy for an exhibit.**

17 Q. Is it a PDF file?

18 **A. I do have a PDF, but I don't know if I'm**
19 **allowed to share that, based on the copyright**
20 **agreements that I have signed.**

21 Q. That's okay. Could you please upload in
22 the Zoom just the table of contents, which includes
23 the topics you read from?

24 **A. I can try to do that.**

25 Q. Thank you. And, Renee -- Court Reporter,

1 let's label that as Exhibit 1.

2 (Exhibit 1 was marked for
3 identification.)

4 Q. (By Ms. Shi) If you could --

5 Dr. Goodrich, for that table of contents, if you
6 could also include the cover page and the copyright
7 page, just the initial part, that will be great.
8 Thank you.

9 **A. All right. Let me see if I can do that.**
10 **For some reason, I'm not able to submit to the chat**
11 **window.**

12 MR. FISHBACK: Dr. Goodrich, if you want
13 to e-mail it to me, I will e-mail it over to
14 Ms. Shi and the court reporter.

15 THE WITNESS: Okay. This might take a few
16 minutes, but let me prepare that.

17 MR. FISHBACK: Whatever is easier.

18 THE WITNESS: Yeah, I can do that right
19 now. It shouldn't take more than two minutes.
20 (Discussion off the record.)

21 THE WITNESS: Okay. I've just sent that
22 to Mr. Fishback.

23 MR. FISHBACK: All right. And I will
24 forward it as soon as I get it.

25 Q. (By Ms. Shi) So what key concepts of

1 social engineering do you address in your computer
2 security class?

3 **A. I talk about generally social engineering**
4 **as a concept, where, in addition to the topics of**
5 **security, we now talk about how people can use things**
6 **that appear to be legitimate, or use subterfuge of**
7 **other kinds to trick people into doing insecure**
8 **actions, such as revealing their user name and**
9 **password, or other credentials, or downloading**
10 **malicious software without realizing it. These kinds**
11 **of things.**

12 **Q. Do you cover phishing?**

13 **A. That is my recollection, that we do cover**
14 **phishing.**

15 MR. FISHBACK: And for the record, I'm
16 sorry to interrupt, it's phishing, P-H, not
17 F-I-S-H-I-N-G. I just see that in the
18 transcript.

19 MS. SHI: Thank you for the clarification.
20 Correct. That is what I'm referring as
21 phishing.

22 **Q. (By Ms. Shi) And so, Dr. Goodrich, sorry,**
23 **I didn't ask you earlier. Is it correct that you**
24 **don't have your e-mail applications open; is that**
25 **correct, on your computer?**

1 **A. No, that's incorrect. I would not be able**
2 **to e-mail the file you just requested if I did not**
3 **use my e-mail system. You asked me to -- literally,**
4 **you just asked me to use my e-mail just a minute ago.**

5 Q. Do you have -- do you communicate, in
6 addition to sending this exhibit to your counsel?

7 **A. No.**

8 Q. Do you --

9 **A. Sorry to interrupt.**

10 Q. I would like to ask you to close the
11 e-mail applications.

12 **A. Okay. It is now closed.**

13 Q. Thank you. And do you have other
14 messaging or communication applications on your
15 computer, other than Zoom, that is open?

16 **A. No.**

17 Q. Thank you.

18 MR. FISHBACK: And, Ms. Shi, I just sent
19 the exhibit over. It might hang up in our
20 e-mail for a second, but it should be on the
21 way.

22 Q. (By Ms. Shi) Could you confirm, other
23 than Zoom, you don't have other applications running
24 open on your computer?

25 **A. I also have Adobe Acrobat open, so that**

1 **you can view the exhibits and documents. I believe I**
2 **also have the finder application, so that I can find**
3 **the exhibits on my hard drive. I believe that's it.**

4 Q. Could you please confirm you don't have
5 Internet browser open?

6 A. **That is correct.**

7 Q. And for your PDF browser, can you confirm
8 that you don't have documents other than your '512
9 declaration open?

10 A. **I still have my textbook open. Would you**
11 **like me to close that?**

12 Q. Yes, please.

13 A. **Okay, I'm closing my textbook.**

14 Q. So in addition to phishing, what other
15 types of social engineering tactics did you discuss
16 in your class?

17 MR. FISHBACK: Objection, form.

18 THE WITNESS: May I reopen my textbook to
19 answer your question?

20 Q. (By Ms. Shi) We need to -- is it -- you
21 can open the table of contents that you sent to us,
22 because the portion you relied upon will be -- need
23 to be part of the exhibit.

24 A. **Right. But now you're asking me about**
25 **other parts of the textbook. That's what I'm**

1 confused about. Maybe the best way to answer is, I
2 include topics that are there in the table of
3 contents. And if you have any other questions about
4 that, I will try my best to remember, but I've been
5 told that a deposition is not a memory test.

6 Q. Yes, that would be -- yes, please answer
7 the question without consult the textbook.

8 A. Yeah, so just as I sit here today, I
9 already -- I already answered that question. I would
10 answer it the same way I did before.

11 Q. Which is --

12 [Cross-talking.]

13 THE WITNESS: The same way I did before.

14 Yeah, could you please have the court reporter
15 read my answer back?

16 MS. SHI: Court Reporter, could you please
17 read Dr. Goodrich's previous response?

18 (Discussion off the record.)

19 Q. (By Ms. Shi) Dr. Goodrich, were you
20 referring to your response to my question that --

21 MR. FISHBACK: Objection -- sorry.

22 Q. (By Ms. Shi) Let me start with your
23 previous response. And, Dr. Goodrich, please tell me
24 if this is the answer you're referring to. You said,
25 "right, but now you're asking me about other parts of

1 the textbook." Is that part of your answer that you
2 were referring to?

3 A. No. What I was referring to is you had
4 asked me about what topics -- as I recall, you had
5 asked me about what topics of social engineering I
6 had taught. And I had mentioned that, generally, the
7 concept of social engineering is to use social cues
8 and contexts to trick people into revealing
9 confidential or sensitive information.

10 Examples include phishing, P-H-I-S-H,
11 other kinds of disguises to trick people into
12 thinking, for example, that websites are legitimate.
13 And then have them reveal confidential information or
14 download malware as a result of them being tricked.

15 The crucial aspect of social engineering
16 is that it circumvents cryptographic or computer
17 security techniques by tricking somebody into doing
18 something that is insecure, rather than actually
19 breaking a cryptographic system or computer security
20 software.

21 Q. Do computer systems -- scratch that.

22 How do you discuss in your class how to
23 recognize and defend against social engineering
24 attacks?

25 MR. FISHBACK: Objection, form.

1 THE WITNESS: I don't recall the details,
2 but my recollection is to tell the students to
3 do their best to verify that websites are
4 legitimate, the e-mail attachments are
5 legitimate, to not click on things unless they
6 know the sender, and verify that the sender is
7 legitimate.

8 These are all general principles that can
9 be applied, but even then -- as the computer
10 security researchers often acknowledge, even
11 then, there may be ways to trick people using
12 social engineering techniques, even when they're
13 trying to be diligent.

14 Q. (By Ms. Shi) So in addition to this human
15 awareness prevention, do you also teach students
16 technical solutions to defend against social
17 engineering?

18 MR. FISHBACK: Objection, form.

19 THE WITNESS: I don't recall, just sitting
20 here today.

21 Q. (By Ms. Shi) Are you aware of technical
22 solutions for defending against social engineering?

23 A. **So in my declarations, I discuss a prior**
24 **art reference known as Kesanupalli, that includes a**
25 **technical solution to protect against social**

1 **engineering.**

2 Q. Which parts -- is any specific
3 technologies described there, that is used to defend
4 social engineering?

5 MR. FISHBACK: Objection, form.

6 MS. SHI: Yeah, let me rephrase my
7 question.

8 Q. (By Ms. Shi) What specific technologies
9 are described in Kesanupalli that are used to defend
10 social engineering?

11 A. So I speak to this in my report, or my
12 declaration, rather, with example for the '512 and
13 the '138 patents, in several paragraphs -- let me
14 just try to list some of them.

15 Yeah, so, for example, in my declaration
16 for the '512 patent, this discussion begins in
17 paragraph 33, goes through paragraph 34. Then it
18 picks up again in paragraph 45, goes through
19 paragraph 60. That's at least inclusive of those
20 discussions. I can read them, if you'd like.

21 Q. So, yeah, let's go to paragraph 33 of your
22 declaration for '512. Can you read the first
23 sentence?

24 A. What paragraph again?

25 Q. 33?

1 **A. Yes. "Kesanupalli states that passwords**
2 **are typically used to authenticate user identity in**
3 **authentication systems and procedures."**

4 Q. So is it right that passwords is one
5 technique to defend against social engineering?

6 MR. FISHBACK: Objection, form.

7 THE WITNESS: That depends on the context.

8 Q. (By Ms. Shi) Could you please explain how
9 it depends on the context?

10 **A. Passwords are used in a wide variety of**
11 **applications, so it depends on the context whether or**
12 **not they're also being used in the context to defend**
13 **against social engineering.**

14 Q. Could you please give one --

15 **A. In the case of Kesanupalli, Kesanupalli is**
16 **advocating for longer passwords, as I explained in**
17 **paragraph 33 of my declaration.**

18 Q. Is it correct that longer passwords is a
19 technique for defend against social engineering?

20 **A. Again, that also depends on the context.**
21 **Generally speaking, longer passwords are considered**
22 **more secure than shorter passwords. And then in**
23 **Kesanupalli, there's a system that is taught that**
24 **shows how you can use longer passwords to defend**
25 **against social engineering attacks.**

1 Q. Could you explain how Kesanupalli uses
2 longer password to defend against social engineering
3 attacks?

4 A. Sure. At a high level, Kesanupalli is
5 about educating users to use longer passwords, but
6 recognizes that the use of longer passwords is
7 difficult, because they're hard to remember.

8 So it discloses a system where there's a
9 fingerprint sensor that is used to help unlock the
10 longer passwords that go with the user ID, so people
11 can log in to a website more securely.

12 And most importantly, Kesanupalli teaches
13 a binding between the credentials for a website and
14 the website itself. And this also protects against
15 social engineering attacks, because it prevents
16 someone revealing their credentials to another
17 website that might look like a legitimate one, but
18 really is not.

19 Q. Is it correct that a longer password is a
20 technique that can be used to improve computer
21 security, other than from social engineering attacks?

22 A. So if your question is, do longer
23 passwords generally give higher levels of security,
24 that is correct. Because as I also talk about, as I
25 recall, in my declaration, there are what are known

1 as dictionary attacks that can be used to break
2 security when people use very short passwords,
3 because those passwords may appear in a password
4 dictionary.

5 Q. So does dictionary attacks trick people as
6 social engineering did?

7 A. No, not usually. Sometimes maybe, but
8 typically not. A dictionary attack is what can be
9 used against weak passwords, hence the advocating for
10 longer passwords in Kesanupalli. And then that's
11 built into its system for preventing social
12 engineering attacks.

13 Q. Are you aware of any other techniques that
14 can be used to defend against social engineering?

15 A. There may be others, but not immediately
16 coming to mind right now, but, yeah, there's probably
17 others.

18 Q. What are the techniques described in the
19 '51 [sic] patent that is used to defend against
20 social engineering?

21 A. When you ask about the '512 patent, are
22 you asking about its claims or its specification?

23 Q. Both.

24 A. So one of the techniques that the '512
25 patent describes to help guard against all attacks,

1 including social engineering, is it teaches against
2 password reuse and/or the selection of poor quality
3 passwords, which render their credentials less secure
4 against attacks.

5 This is, for example, from the background
6 section of the '512 patent, in column 1, beginning at
7 line 35, and going to line 44.

8 Q. Is it correct that the technique you just
9 described in '512 of against -- teaching against
10 password reuse or selection of poor quality passwords
11 are not limited to defend against social engineering
12 attacks?

13 A. I agree.

14 Q. Any other techniques in the '512 patent
15 that are described to guard against social
16 engineering attacks?

17 A. If by your question, you're asking
18 specifically for just social engineering attacks,
19 nothing else is immediately coming to mind. But of
20 course, the claims of the '512 patent would be
21 recognized by a person of ordinary skill in the art
22 as providing improved computer security, generally.

23 Q. And would the claims of '512 be recognized
24 by a person of ordinary skill in the art as providing
25 improved computer security specific for social

1 engineering attacks?

2 **A. I don't recall that being a question I was**
3 **asked to opine on. I would want to spend more time**
4 **to be able to answer that question.**

5 MS. SHI: Okay. We're close to one hour
6 in the deposition. Can we take a ten-minute
7 break?

8 MR. FISHBACK: Fine here.

9 THE WITNESS: Yeah, that's fine with me.

10 MS. SHI: Thank you.

11 (A recess was taken.)

12 Q. (By Ms. Shi) So we were talking about the
13 '51 [sic] patent. Can you please -- do you have the
14 '51 -- '512 patent in front of you?

15 **A. I do.**

16 Q. Can you go to figure 1, please?

17 **A. I am there.**

18 Q. So could you please describe figure 1?

19 **A. Sure. So figure 1 is an illustration of**
20 **an embodiment of an environment in which the**
21 **authentication translation system disclosed in the**
22 **'512 patent is provided.**

23 Q. So where is the authentication translator
24 module is -- in which device is the authenticator
25 translator module is in?

1 MR. FISHBACK: Objection, form.

2 THE WITNESS: So if we go to the

3 '512 patent, in column 3, and beginning at line
4 2, it explains that "also, as will be described
5 in more detail below, authentication translators
6 can be located in a variety of places within an
7 environment. For example, notebook computer 102
8 includes an authentication translator module 132
9 that provides authentication translation
10 services. Other devices 104 to 108 can also
11 include, but need not include, their own
12 respective authentication translator modules."

13 Q. (By Ms. Shi) So is it right that the
14 device 102 communicates -- can communicate with all
15 the other devices on figure 1, including social
16 networking site 120, bank website 122, online camera
17 retailer 124, cloud storage service 140, third-party
18 authentication translator 136; is that correct?

19 A. So if we go column 2 in the '512 patent,
20 beginning at line 37, it says, "figure 1 illustrates
21 an embodiment of an environment in which
22 authentication translation is provided. In the
23 examples shown, a variety of client devices 102 to
24 108 connect via one or more networks represented as a
25 single network cloud 110 to a variety of services 120

1 to 124, also referred to herein as sites 120 to 124."

2 So those are at least inclusive of the
3 other sites that can be communicated with through
4 that network.

5 Q. So you discussed 120 to 124. What about
6 140 cloud storage service, how does the device 102
7 communicate with cloud storage service 140?

8 A. So if we go to column 7, beginning at line
9 60, it states, "Alice's laptop 102 and phone 104
10 could both communicate with cloud storage service
11 140, which would keep their authentication
12 information synchronized."

13 Q. So what's the use of cloud storage service
14 140 here?

15 A. In this case, it's talking about keeping
16 their authentication information synchronized. And
17 then it goes on, at line 62, "refreshes can also be
18 made in accordance with user configuration
19 restrictions. For example, Alice's employer could
20 prevent privileged employer data from being stored on
21 shared personal devices or on any device that was not
22 issued by the employer."

23 Q. Okay. So in this case, is it correct that
24 the privileged employer data is stored on cloud
25 storage service 140?

1 MR. FISHBACK: Objection, form.

2 THE WITNESS: That is not being disclosed
3 here. It may be a possible embodiment, but
4 that's not what's being disclosed.

5 Instead, what it's saying is that Alice's
6 employer could prevent privileged employer data
7 from being stored on the shared personal devices
8 or any device that was not issued by the
9 employer.

10 Q. (By Ms. Shi) Can you read the first
11 sentence of this paragraph, starting with "in various
12 embodiments"?

13 A. Yes, it says -- beginning in line 56 of
14 column 7, "in various embodiments, cloud storage
15 service 140 is configured to accept backups from
16 multiple devices associated with a single account,
17 and synchronize the updates, so that all devices get
18 automatically refreshed."

19 Q. What does "accept backups" mean here?

20 A. A person of ordinary skill in the art
21 would understand that to mean just what it says, that
22 you could accept backup of data that, say, is stored
23 on Alice's laptop 102, and then could be backed up to
24 this cloud storage service 140.

25 Q. Is it right that the backup is sent from

1 Alice laptop 102 through the Internet, and then
2 accepted by the cloud storage service 140?

3 A. It depends what you mean by sent, because
4 claim 1 speaks of there being a first processor and a
5 second processor. So if now you're asking about
6 claim language, you have to be a little more careful.

7 Also, I don't see any language here at
8 least in this thing about the acceptance or rejection
9 of a backup. So I'm not -- I'm not seeing that here.
10 It may be somewhere else, if you -- if you would be
11 willing to point me to another section in the patent,
12 I'd be happy to review that.

13 Q. In the sentence you just read, it says,
14 "cloud storage service 140 is configured to accept
15 backups"?

16 A. Right. But the way you asked the question
17 suggested that it could also reject them, so that was
18 the part I was responding to.

19 Q. So you don't disagree that cloud storage
20 service 140 can accept backups from multiple devices
21 through Internet; is that right?

22 MR. FISHBACK: Objection, form.

23 THE WITNESS: There are multiple
24 embodiments. If now you're asking about other
25 embodiments that may not be in claim 1, I would

1 not dispute that there may be other embodiments,
2 besides what is in claim 1.

3 Q. (By Ms. Shi) So let's read this sentence
4 again. I'm not asking this question related to
5 claim 1. Just to clarify, I'm focused on this
6 sentence you read that's from column 7, line 56.
7 Could you please read that first sentence?

8 A. Sure. Again, it says, beginning at line
9 56, "in various embodiments, cloud storage device 140
10 is configured to accept backups from multiple devices
11 associated with a single account, and synchronize the
12 updates, so that all devices get automatically
13 refreshed."

14 Q. Can this sentence -- what's described in
15 the sentence implemented in figure 1?

16 MR. FISHBACK: Objection, form.

17 THE WITNESS: So, again, figure 1 is not a
18 flowchart, like steps or even a data flow
19 diagram that would show the flow of data which
20 are in this patent.

21 So, for example, figure 6, figure 7 are
22 data flow diagrams. And then figure 5 is a
23 flowchart showing logical flow. Instead,
24 figure 1 would be understood by a person of
25 ordinary skill in the art to be an illustration

1 of an architecture that shows the potential
2 connections that could exist in a system, and is
3 meant to illustrate how, for example, a laptop
4 could be connecting to a bank.

5 Q. (By Ms. Shi) You mentioned claim 1
6 recites a first processor and a second processor; is
7 that right?

8 A. Yes, that is correct.

9 Q. Does the architecture of figure 1 include
10 a first processor and a second processor as recited
11 in claim 1?

12 MR. FISHBACK: Objection, form.

13 THE WITNESS: So figure 1 is just an
14 illustration of the devices and the websites and
15 cloud components. Instead, if you want to see
16 an architecture diagram that shows a first
17 processor and a second processor, an example
18 would be figure 3.

19 Q. (By Ms. Shi) What is figure 3?

20 A. So figure 3 is an illustration of an
21 embodiment of a device which secures storage. And it
22 shows both a first processor and a second processor.
23 The first processor is numbered 304, the second
24 processor is number 308.

25 Q. Can the embodiment of the device

1 illustrated in figure 3 implemented in device 102 of
2 figure 1?

3 A. A person of ordinary skill in the art
4 would understand that that could be done. That would
5 be possible.

6 Q. So is there communication between the
7 processors 304 and 308 in figure 3?

8 A. If you're asking about the preferred
9 embodiment of how -- what figure 3 is illustrating,
10 that's discussed, for example, beginning in column 3,
11 starting at line 66, and then continuing into
12 column 4. And one of the disclosures begins at
13 line 5. It says, "however, users cannot access the
14 secure storage area, and the fast processor can only
15 communicate with the dedicated processor/sensor via a
16 restricted API."

17 Q. Is it correct that the dedicated processor
18 sensor is 308?

19 A. Yes, because if we look just to the part
20 before that, it says, beginning at line 66 of
21 column 3, "one example of a device with secure
22 storage is illustrated in figure 3. In the example
23 shown, a mobile phone 300 includes a large and
24 insecure storage 302 attached to a fast processor
25 304, and a smaller but secure storage 306 attached to

1 **a dedicated processor 308 and a sensor 310, e.g., a**
2 **camera or fingerprint reader."**

3 Q. So can a processor 304 communicate
4 directly to the Internet?

5 MR. FISHBACK: Objection, form.

6 THE WITNESS: If by communicate directly
7 with the Internet, you mean can that processor
8 be used by a user to access an external resource
9 across the Internet and establish a secure
10 connection with that external source, the answer
11 is yes.

12 Q. (By Ms. Shi) Can the user do the same
13 with the processor 308?

14 A. No. As I read earlier, at line 5 of
15 column 4, it states, "however, users cannot access
16 the secure storage area, and the processor can only
17 communicate with the dedicated processor/sensor via
18 restricted API."

19 And then, of course, that -- it goes on in
20 this passage to talk about how the secure processor
21 can communicate with other entities, but then that is
22 not the user doing that anymore. It's now the secure
23 processor doing it in response to perhaps a
24 communication through the restricted API.

25 Q. So the processor 308 can communicate with

1 other entities, but it needs to go through the
2 restricted API; is that right?

3 MR. FISHBACK: Objection, form.

4 THE WITNESS: Not exactly, no. Instead,
5 what is being taught here is that the secure
6 processor -- that the user and the fast
7 processor 304 have restrictions in how they
8 interact with the secure processor. Namely,
9 they must use this restricted API.

10 But then in this passage in column 4,
11 which then supports the claim language, say, for
12 claim 1, it's disclosing how the secure
13 processor can communicate, for example, with a
14 backup storage service 140 to do a backup.

15 Q. (By Ms. Shi) So in your class on computer
16 security, how do you define security?

17 A. Yeah, so if we go to the table of contents
18 for the book that we now are sharing, and I'm
19 presuming will become an exhibit for this deposition,
20 if we go to the introduction, we see where we
21 discuss -- this is not the text, but this is now the
22 table of contents.

23 We discuss security principles,
24 fundamental concepts. So the concept of computer
25 security is wrapped up into a number of other

1 **sub-concepts. The first three go by the initials**
2 **CIA, which stands for confidentiality, integrity, and**
3 **availability. And each of those concepts are**
4 **concepts of computer security.**

5 And then we also, in our book, introduce
6 **three additional ones, which go by AAA, which deal**
7 **with assurance, authenticity, and anonymity. So**
8 **those concepts also relate to computer security. And**
9 **these are all things that I teach when I teach my**
10 **course on computer security as being security**
11 **concept.**

12 Q. So is it correct that the security of a
13 system has the goals of integrity, confidentiality,
14 and availability?

15 MR. FISHBACK: Objection, form.

16 THE WITNESS: Those are three
17 subcomponents of what it can mean to be
18 security. So some systems may provide one or
19 more of those as its goals.

20 Q. (By Ms. Shi) Can a system have all three
21 of them, integrity, confidentiality, and
22 availability, as its goals?

23 A. Yes, that is possible, as well as the
24 other goals we discussed as well, assurance,
25 authenticity, and anonymity.

1 Q. What is confidentiality?

2 A. Confidentiality is the concept that some
3 data is kept and stored and transmitted in a way that
4 it is kept confidential, so that only people who have
5 the access rights to that data may see it.

6 And those access rights may be embodied,
7 for example, in some type of a secret key, which is a
8 number or password that can unlock the data through
9 some cryptographic means, for example.

10 Q. Other than the secret key you mentioned,
11 are there additional tools for implementing
12 confidentiality?

13 A. Yes, there's another tool known as public
14 key cryptography. In this case, rather than just
15 having a shared secret key between the two parties,
16 an entity, such as -- we'll call it Bob has a private
17 key that only he knows, and a public key that he
18 publishes widely to everyone.

19 And then if another party, who we'll call
20 Alice, wishes is to send a confidential message to
21 Bob, she can encrypt it using his public key, which
22 is known to everybody. But then after she sends it,
23 or even during transit, anyone else who looks at
24 that -- what we call a cipher text will not be able
25 to determine its value, its true identity.

1 But then once Bob gets it, he can use his
2 private key to decrypt that data, so that he can read
3 it.

4 Q. Is authentication also a tool for
5 confidentiality?

6 MR. FISHBACK: Objection, form.

7 THE WITNESS: Authentication can be used
8 in conjunction with confidentiality, but it,
9 just by itself, is not a tool for
10 confidentiality. It's instead a tool for
11 authenticating that somebody is who they say
12 they are.

13 There may be confidential components to
14 any protocol that you do to achieve
15 authenticity, but the concept itself is simply
16 that. Determine that somebody or something is
17 what they say they are. That's authentication.

18 Q. (By Ms. Shi) Any other tools for
19 confidentiality?

20 A. Another tool that can be used for
21 confidentiality is cryptographic hash functions,
22 where you take data, and you run it through this hash
23 function that then produces an output that we
24 referred to as being one way.

25 And what that means is that the output of

1 that function is hard to invert. It's easy to
2 compute in one direction, but it's hard to invert.
3 Namely, that if you're given the output from a
4 cryptographic hash function, it's computationally
5 difficult to reverse that and find an input value
6 that would have that output.

7 Q. Any other tools for confidentiality?

8 A. There may be others. They're not
9 immediately coming to mind, as I sit here today.

10 Q. What is integrity?

11 A. Integrity has to do with the property that
12 the data is unchanged from when it was created. That
13 it's true, has not been altered. So this is
14 different than confidential information. This is
15 information that could be shared with others, but you
16 want to make sure that it has not been altered, say,
17 by some hacker who would be introducing a virus into
18 some software, for example. You'd like to make sure
19 that the software has integrity, that it is as it was
20 originally released, for example.

21 Q. What are tools for integrity?

22 A. So example tools in use today for
23 integrity include digital signatures. So the idea
24 there is that perhaps using this public key, private
25 key mechanism we talked about earlier, that an

1 entity, which we'll call Bob, will digitally sign,
2 say, software data. And then send that software
3 together with a digital signature to someone like
4 Alice. And then she can verify that that message was
5 the same that Bob signed by doing a signature
6 verification on that.

7 Q. Are there other tools for integrity?

8 A. Yes.

9 Q. What are they?

10 A. Another tool is something called an HMAC,
11 or we pronounce it as HMAC. This is now in a
12 scenario where two individuals, for example, Alice
13 and Bob, may share a secret key. In this case, what
14 you can do is, you can take that original message,
15 run it through a cryptographic hash function, where
16 you concatenate the message with a secret key, and
17 provide that as input to the cryptographic hash
18 function.

19 And then send the message together with
20 this HMAC to the other party, who also knows that
21 secret key. So then they can take the message that
22 was sent, concatenate the secret key, compute the
23 one-way hash function on that, and then compare that
24 to the hash value that was also sent. If they match,
25 then this is evidence of integrity.

1 Q. Any other tools for integrity?

2 A. Those are two that are immediately coming
3 to mind. There may be others that I'm just not
4 recalling, as I sit here today.

5 Q. What is availability?

6 A. So availability is the property that data
7 or a system is available, that people who want to,
8 say, connect to a website and download the web page
9 are able to do that.

10 Q. What are some tools for availability?

11 A. So tools for availability include
12 redundancy, where you would take a website or web
13 server, and rather than just having one web server,
14 you'd have multiple copies of that web server. So
15 that if one of them goes down, then the other can
16 take over the functionality of that web server. And
17 that general web page would still be available.

18 Q. Are there any other tools for
19 availability?

20 A. Another tool for availability is the
21 prevention of denial of service attacks. So somebody
22 who is trying to attack a system by overloading it
23 with requests is trying to attack its availability.
24 So tools that, then, would be preventing denial of
25 service attacks would be tools that benefit

1 **availability.**

2 Q. So defending against social engineering
3 attacks helps with which of these goals?

4 MR. FISHBACK: Objection, form.

5 THE WITNESS: It helps with at least
6 confidentiality and integrity.

7 Q. (By Ms. Shi) So Exhibit 1 to this
8 deposition, which is the table of contents of the
9 book, your book, Introduction to Security [sic],
10 chapter 2 says, "physical security." What is
11 physical security?

12 A. **Physical security is the actual physical**
13 **protection of computing devices. So, for example,**
14 **keeping them in locked rooms and in data centers that**
15 **have physical access controls, so that only**
16 **authorized people can go into the room.**

17 Q. Why is physical security important for
18 achieving the security goals?

19 A. **Because oftentimes, if someone can get**
20 **access physically to computers, they can disassemble**
21 **them, which affects availability. They can turn them**
22 **off, which affects availability. They could**
23 **potentially even open them up and put in probes.**
24 **They could compromise confidentiality or they could**
25 **introduce new data and change things that would**

1 **compromise integrity.**

2 Q. Does physical security help to defend
3 against social engineering?

4 A. We have a section in this chapter on human
5 factors and social engineering, but it was actually
6 addressing the opposite question, how can you build
7 physical security systems that prevent against social
8 engineering, such as somebody being tricked into
9 giving their key card to an attacker, and then the
10 attacker uses their key card to gain access to a data
11 center.

12 Q. So physical security can be used to defend
13 against a variety of attacks, including social
14 engineering attacks; is that right?

15 A. I don't -- again, I wouldn't put it that
16 way per se. I think the way to say it is, you would
17 like to have physical security means that are
18 difficult to thwart through social engineering
19 attacks.

20 So, for example, in this example of having
21 a key card, you could have on the key card, a
22 physical picture of the person. So that if they
23 handed that to a third-party through coercion or
24 whatever social engineering was used, that then when
25 that third-party shows their key card to the reader

1 **and their face doesn't match, or a guard can see the**
2 **picture doesn't match, then they will be caught.**

3 MR. FISHBACK: And I'm sorry to interrupt.
4 Is anyone else having connection issues or any
5 lagging?

6 (Discussion off the record.)

7 Q. (By Ms. Shi) You mentioned that it is
8 desirable to have physical security means that are
9 difficult to thwart through social engineering
10 attacks, do you recall?

11 A. **I don't think I said thought through.**

12 Q. What did you say?

13 A. **I thought difficult to attack, something**
14 **along those lines. I think I said thwart, actually.**

15 Q. Are there needs for physical security
16 means that are difficult to --

17 (Discussion off the record.)

18 Q. (By Ms. Shi) Are there physical security
19 means that would be desirable to break through, other
20 than social engineering attacks?

21 A. **When you say break through is desirable,**
22 **you're now taking the perspective of an attacker; is**
23 **that correct.**

24 Q. Let me rephrase. Are there physical
25 security means that would be desirable that is

1 difficult to break through?

2 MR. FISHBACK: Objection, form.

3 Q. (By Ms. Shi) Other than social
4 engineering attacks?

5 MR. FISHBACK: Same objection.

6 THE WITNESS: Yes, so we also talk about
7 locks and safes in this chapter, so we talk
8 about how to build locks that are difficult for
9 someone to pick them. That is to be able to
10 unlock the device or the safe without knowing
11 the combination or having a physical key for it.

12 All of this, of course, is not things I
13 discussed in my declaration. I was not asked to
14 opine on these things.

15 Q. (By Ms. Shi) What is operating system
16 security?

17 A. **So an operating system on a computer is**
18 **the software that manages things like the processes,**
19 **the memory, the file system, connected devices. And**
20 **it's generally desirable that the operating system**
21 **itself also be secure, that someone can't introduce**
22 **malicious software into the operating system, for**
23 **example.**

24 Q. What are tools for operating system
25 security?

1 A. So some example tools to achieve operating
2 system security is to have what is known as access
3 control restrictions, so that the software of the
4 operating system itself can only be modified by
5 system administrators, for example. That's one tool.

6 Other tools are that you build the
7 operating system itself to be robust against attacks
8 that could be trying to break those restrictions or
9 other restrictions that the operating system is
10 trying to enforce.

11 Q. In the table of contents, 3.2, you
12 discussed process security. What is process
13 security?

14 A. So in a computer system, running threads
15 of computer software are known as processes in the
16 context of an operating system. And so what you'd
17 like to do is to protect the processes that are
18 running in an operating system.

19 So, for example, each process will
20 typically have a memory space that is associated with
21 it. And it's desirable, generally, that the memory
22 for one process is not accessible to another process
23 unless that first process gives explicit rights for
24 the other process to access that memory.

25 So, for example, you'd want to have

1 **protections in place to prevent this leakage from one**
2 **process's memory to another process's memory.**

3 Q. Is operating system security used to
4 defend against social engineering attacks?

5 A. No examples are coming immediately to
6 mind, as I'm sitting here today, but that doesn't
7 mean that they don't exist. I'm just not having any
8 that come up. Again, this whole line of questioning
9 is something that is completely outside the scope of
10 my declaration.

11 Q. Section 3.3 is about memory and file
12 system security. Do you see that?

13 A. Yes.

14 Q. What is memory in a file system security?

15 A. So this gets to the issue that, for
16 example, certain files oftentimes are sensitive, and
17 you would like to restrict who has access to the
18 contents of those files. And so what you can do is
19 to provide through the operating system, mechanisms
20 that protect the contents of files, and only allow
21 those who are authorized to see them or to modify
22 them to do so.

23 Q. What is virtual memory security?

24 MR. FISHBACK: Objection, form, scope.

25 THE WITNESS: So, again, we're going far

1 afield now from my declaration, but in computer
2 science, we oftentimes will give the impression
3 that each process has access to the entire
4 address space of a memory, when, in fact,
5 multiple processes are sharing that memory.

6 To achieve this abstraction for the
7 processes, we use a technique called virtual
8 memory. What this refers to is that the memory
9 space of the process is divided into chunks, we
10 often refer to as pages or segments.

11 And each page is then brought into the
12 actual memory of the computer when that process
13 needs it. But it may be swapped out, say, to an
14 external drive when the process does not need
15 it. And we refer to this technology as virtual
16 memory.

17 Q. (By Ms. Shi) What is the virtual memory
18 security techniques used to prevent -- let me
19 rephrase.

20 What kind of attacks are the virtual
21 memory security tools used to defend against?

22 **A. So --**

23 MR. FISHBACK: Same objections.

24 THE WITNESS: So this, again, is dealing
25 with the issues of protection against someone

1 trying to access data that they are not
2 authorized to see.

3 So what you want to do is both protect the
4 memory when it's inside the computer in the main
5 memory, but also when it's been swapped out to
6 the external drive. And so this virtual memory
7 security techniques would be used to protect the
8 address space of a process, both when it's being
9 used inside the internal memory of a computer,
10 as well as when it has been swapped out to the
11 external memory.

12 This is like office hours. This is so
13 much fun. Thank you for all these wonderful
14 questions, of course, that are completely
15 outside the scope of my declaration for this
16 matter.

17 Q. (By Ms. Shi) So in section 3.4, you
18 listed a few attacks. 3.4.2 says, "simple buffer
19 overflow attacks." What kind of attacks are you
20 discussing here?

21 A. **So this is referring to an attack known as**
22 **a buffer overflow attack. So a buffer in an**
23 **operating system is a piece of memory that's**
24 **allocated for, say, inputs, outputs, communications**
25 **between two entities, could even be a buffer that's**

1 used for a website, for text that's being input into
2 a graphical user interface, that then is processed by
3 the operating system.

4 And what can happen, though, is that an
5 attacker can give an input into the buffer that is
6 bigger than the size of the buffer itself. And this
7 is known as a buffer overflow attack. And then what
8 the attacker can do is by giving it input that's so
9 large, that then the computer that is not defending
10 against a buffer overflow attack will do is it just
11 accepts that, and overwrites memory.

12 But then continues overwriting memory
13 beyond the space of the buffer, which then can damage
14 other memory. And it gets to that issue of damaging
15 memory that you want to otherwise protect.

16 Q. So are these attacks -- scratch that.

17 So the next chapter is malware, and
18 section 4.1 is about insider attacks. Were the
19 attacks we just described in section 3 outsider
20 attacks?

21 A. Not necessarily.

22 Q. So section 3 and 4 can overlap; is that
23 right?

24 A. Yes.

25 Q. So why is insider attacks an issue that

1 computer security need to deal with?

2 A. Because to achieve computer security
3 goals, it's oftentimes useful to limit the access
4 rights of users, and to have roles assigned to the
5 user, such as system administrator, accountant,
6 manager, these kinds of roles in an enterprise.

7 And you want to oftentimes restrict the
8 access, or the types of things each person and these
9 different roles can achieve. But if you have an
10 insider inside your company, let's say, who is
11 actively trying to thwart the security and break it,
12 and introduce issues that are bad, this is something
13 that you should defend against.

14 And this is especially true for the
15 programmers who are programming the software for an
16 enterprise. Those are the ultimate insiders. And so
17 you want to put in place procedures for software
18 development that help reduce the possibility that a
19 programmer could introduce malicious software while
20 they're writing their programs. And that has to do
21 with insider attacks.

22 Q. And the malware attacks can come from
23 insider or outsider; is that right?

24 A. That is correct. This section is about
25 insiders.

1 Q. Section 1.4 is about insiders; is that
2 right?

3 A. **Section 4.1 is about insiders.**

4 Q. Thank you. And is it desirable to have
5 security against malware against both insider attacks
6 and outsider attacks?

7 MR. FISHBACK: Objection, form.

8 THE WITNESS: I would generally agree with
9 that, depending on the system.

10 MR. FISHBACK: Ms. Shi, we've been going
11 for about an hour. When you get a good chance,
12 could we take a break?

13 MS. SHI: Yeah, let's take a ten-minute
14 break.

15 MR. FISHBACK: Awesome. Thank you.

16 MS. SHI: Thank you. Let's go off record.

17 (A recess was taken.)

18 Q. (By Ms. Shi) So before the break, we were
19 talking about chapter 4, malware; is that right?

20 A. **Yes, I recall that.**

21 Q. What is a worm?

22 A. **So a computer worm is software that can**
23 **spread itself without intervention from any human.**
24 **So it can spread itself from computer to computer,**
25 **and infect the computers, and doesn't need a user to**

1 **click on an e-mail. Those kind of things.**

2 Q. So what does a computer worm usually will
3 do?

4 A. **It will try to infect multiple computers**
5 **to then potentially set them up as what we call bots,**
6 **B-O-T-S, where then they can be used for themselves**
7 **to then attack other computers, perhaps do a denial**
8 **of service attack on a website.**

9 Q. What are the tools to -- against worms?

10 MR. FISHBACK: Objection to form, scope.

11 THE WITNESS: Example tools to protect
12 against computer worms are to have improved and
13 robust authenticity and authorization. So, for
14 example, if somebody is logging in to your
15 computer, you want to make sure that they're
16 logging in with correct and valid credentials.
17 And this would then prevent, say, a worm coming
18 in to attack with what would presumably be
19 invalid credentials.

20 Q. (By Ms. Shi) Can signature -- digital
21 signature used to fight against malware?

22 A. **Yes.**

23 Q. How would it work?

24 A. **So, for example, another type of malware**
25 **is something called a computer virus, which is**

1 malicious software that injects itself into other
2 software. And then is sent, say, through e-mails or
3 other means, where people would click on something
4 and then install it, not knowing that it has this
5 virus inside of it.

6 But what you can do to protect against
7 that is that a software designer, such as Microsoft,
8 could digitally sign their software. In fact, they
9 do today digitally sign all their software, so that
10 when you install your software from, say, Microsoft,
11 before you do the installation, you first check that
12 the software has a valid digital signature. And if
13 it does, then that's evidence that it has not been
14 tampered with. Hence, it is unlikely to have a
15 computer virus.

16 Q. So I've -- personally, I've used some
17 antivirus software. Is that a technique pretty
18 commonly used on my device to protect against
19 malware?

20 MR. FISHBACK: Objection, form, scope.

21 THE WITNESS: I don't know how common it
22 is. And, again, we're talking about things
23 today, not in the scope of the patents, but the
24 idea of much of the computer virus software of
25 today, it is doing something called signature

1 checking, which is a -- I have to apologize for
2 my colleagues -- a different type of a signature
3 than a digital signature that's used to sign and
4 protect software, so you know it's from a good
5 source.

6 Here, what we're referring to, in using
7 this word "signature," to be a pattern, that
8 certain viruses tend to have a certain pattern
9 in the actual binary bits of the software. And
10 so we look for a certain pattern of zeros and
11 ones here, a certain pattern of things over
12 there.

13 And that pattern of software that tends to
14 go with certain computer viruses, we call that a
15 signature. But it's a different signature than
16 the digital signature we were talking about
17 earlier today.

18 Q. (By Ms. Shi) So is it correct that the
19 antivirus software installed on my device is using a
20 specific type of --

21 (Discussion off the record.)

22 Q. (By Ms. Shi) So let me ask my question
23 again. How does checking a digital signature of code
24 protect a device?

25 MR. FISHBACK: Objection, form, scope.

1 THE WITNESS: So this what we talked about
2 earlier, what I was referring to earlier.
3 Again, there's this digital signature, where a
4 software developer or a company will digitally
5 sign the software that they release, such as
6 Microsoft releasing its software.

7 So that then, when you install it, you
8 check the digital signature, that this is a way
9 of achieving integrity, that the software that
10 was sent is the same software that you're
11 installing. Hence, it's unlikely to include a
12 computer virus in that software. So that's a
13 technique that's very common today for
14 protecting against computer viruses in
15 distributed software.

16 Q. (By Ms. Shi) So we discussed encryption
17 before. Can we use encrypted -- can we use
18 encryption to fight against malware?

19 A. Yes. So one of the ways that you can
20 do -- you can perform digital signatures is through a
21 type of encryption. We talked earlier about public
22 key encryption, how Bob can have a public key that he
23 shares with everyone. And anyone who wants to
24 encrypt a message for Bob can use that. And then he
25 uses his private key to decrypt that.

1 There are some types of public key
2 cryptography, where those keys can be reversed. Bob
3 can use his private key to encrypt something. And
4 then everybody else can use his public key to decrypt
5 it. And this could then be a form of a digital
6 signature for Bob.

7 You can take his software he just wrote,
8 encrypt it with his private key. Send both that and
9 original unencrypted software to you. And then you
10 will then encrypt the software using his public key,
11 and see if that matches what he had encrypted with
12 his private key, or likewise, you could decrypt his
13 encrypted software, and see that it matches the
14 software he sent you.

15 And this is a form of a digital signature.
16 And something akin to this is used today, in fact,
17 for digital signatures.

18 Q. So can I use encryption in my computer to
19 protect my files?

20 MR. FISHBACK: Objection, form, scope.

21 THE WITNESS: Yes, that's something you
22 can use today. There's a number of tools that
23 are available today to encrypt the files on your
24 computer, say, using a password that you know.

25 And then what that would do is anyone who

1 would then gain access to your computer, who
2 does not know that password or key, they can see
3 the encrypted files on your computer, but they
4 would not be able to either modify them without
5 breaking the encryption, and then it would just
6 be garbage when you tried to decrypt it, or they
7 would not be able to see the unencrypted version
8 of them.

9 Q. (By Ms. Shi) Are there commercially
10 available tools like that?

11 A. **Yes, there are today.**

12 Q. Can you give some examples?

13 A. **Yes. So, for example, on the Mac, the
14 Apple Company provides a tool where you could have
15 all of your files on your hard drive encrypted, if
16 you'd like. And then there's other third-party
17 software that does similar things.**

18 **In fact, it was with -- working with law
19 firms that I discovered some of these that are being
20 used today, 'cause oftentimes, law firms will want to
21 protect the software of their clients. And then only
22 send that on a flash drive that is protected using
23 one of these third-party tools.**

24 Q. I think we discussed access control a
25 while back. Is it correct that providing different

1 levels of access control is another way to provide
2 protection of the device?

3 MR. FISHBACK: Objection, form, scope.

4 THE WITNESS: Generally speaking, today,
5 that's another tool that is being used to
6 protect sensitive data. That if you don't have
7 access rights to the data, then the operating
8 system should have mechanisms in place to
9 prevent you from getting at the data.

10 Q. (By Ms. Shi) Are you aware of other tools
11 for protecting sensitive data?

12 A. We already talked about encryption.
13 Encryption and access controls are probably the most
14 widely used today. I'm not thinking of any other
15 examples, as I sit here today.

16 Q. The next chapter, chapter 5 is titled
17 "network security, 1." Do you see that?

18 A. Yes.

19 Q. Of your book table of contents, Exhibit 1
20 of this deposition. Why is network security
21 important for computer security?

22 MR. FISHBACK: Objection, form, scope.

23 THE WITNESS: So generally speaking,
24 today, computers are connected through networks
25 to oftentimes perform operations, do

1 communications of various types. Hence,
2 protecting the network that the computers use
3 and that the -- the protocols that occur in the
4 network is also protecting both the computers
5 and their data as well.

6 Q. (By Ms. Shi) Is it correct that
7 encryption is a technique that can be used to
8 increase network security?

9 **A. Yes, encryption is used in some cases**
10 **today for achieving various goals of network**
11 **security.**

12 Q. How does that work?

13 MR. FISHBACK: Objection, form, scope.

14 THE WITNESS: There's a number of ways
15 that encryption is used. So probably the most
16 common, actually, technically, is something that
17 we discuss in chapter 6 is when you go to a
18 web page nowadays, you typically are going to
19 use a protocol called HTTPS.

20 And what this does is when you use this
21 protocol, it encrypts the session you have
22 between your computer and the website, so that
23 all the packets that are being sent between them
24 are encrypted, the data in them is encrypted.
25 So if anyone were to eavesdrop on your

1 communication, say, through your wifi, they
2 would not learn the contents of those packets,
3 the data portion.

4 Q. (By Ms. Shi) Can the transmission -- the
5 security of the transmission of the data be improved
6 by using multilayer of encryption? For example, I
7 encrypt it first before I send it on to network, and
8 then use the HTTPS protocol to communicate that
9 encrypted data?

10 MR. FISHBACK: Objection, form, scope.

11 THE WITNESS: That one is a more slippery
12 slope today, unfortunately. Namely, one of the
13 ways that attackers now are introducing computer
14 viruses on to computers is to be sending them
15 through encrypted sessions, such as with HTTPS.

16 And so what some systems are doing to
17 protect against that is that they are inside of
18 a processor known as a proxy. They will decrypt
19 the packets, check them for a computer virus,
20 and then re-encrypt them using HTTPS back to
21 send it back to you.

22 And so encrypting inside of an HTTPS
23 protocol can protect data when you know what
24 you're doing, but it could also potentially be
25 hiding a computer viruses that your proxy might

1 not catch. That's a problem that exists today.

2 Q. (By Ms. Shi) So there are techniques
3 using encrypted data for transmission, and there are
4 techniques that communicate using unencrypted data;
5 is that right?

6 A. Generally speaking, there's things that
7 can use encrypted data, and there's things that can
8 use unencrypted data, yes. That's a very broad
9 question. And various techniques exist today for
10 that.

11 Q. So in the network sections 5 and 6, you
12 have listed many types of attacks. Do you see those?

13 A. Yes.

14 Q. Are those attacks mainly attacking the
15 content that is communicated -- sorry, scratch that.
16 Are those attacks -- the attacks described
17 in sections 5 and 6 directed at the cloud portion of
18 a network, instead of attacking the end devices?

19 MR. FISHBACK: Objection, form, scope.

20 THE WITNESS: No, I would not characterize
21 it that way. Instead, the way that we wrote
22 these two sections was organized, based on
23 something known as the network stack, which is a
24 set of layers of how networks are designed
25 starting with the hardware at the bottom layer.

1 And then going up to the applications at the top
2 layer.

3 And what we talk about in these chapters
4 are attacks that can occur at every layer. Some
5 of those attacks are attacking the protocols
6 themselves, and trying to achieve denial of
7 service. Some of those attacks are trying to
8 hijack a communication. Some of them are about
9 eavesdropping on communications. There's a
10 whole variety of possible attacks that we talk
11 about in these chapters.

12 Q. (By Ms. Shi) Can you give one example
13 that attacks the end user computer, instead of
14 attacking the Internet devices?

15 MR. FISHBACK: Objection, form.

16 THE WITNESS: Sure. So in section 6.4.4,
17 we talk about an attack known as port scanning.
18 This, at first, might seem like it's not even an
19 attack, but it potentially is setting up another
20 attack.

21 So what this refers to is how an attacking
22 computer can scan the various ports on your
23 computer, to see which of them are accepting
24 connections. And in some cases, if you are
25 accepting connections on certain ports, and you

1 may even be using old software to accept those
2 connections, then an attacker can then do an
3 intrusion attack on your computer through that
4 port. That's a risk that exists today, for
5 example.

6 Q. (By Ms. Shi) Is it correct that network
7 security is tied pretty closely with web security
8 taught in section 7?

9 MR. FISHBACK: Objection, form, scope.

10 THE WITNESS: Actually, no, as it turns
11 out. I mean, technically, in order to connect
12 to a website, you have to go through the
13 network. But then what we're talking about here
14 in chapter 7 is the security of websites
15 themselves. So the software that's running on
16 the website itself, how do you protect the
17 servers. These kinds of things.

18 Q. (By Ms. Shi) So web security is really
19 about protecting the devices, while network security
20 is more broadly directed at the network connections;
21 is that correct at all?

22 MR. FISHBACK: Objection, form, scope.

23 THE WITNESS: No. Actually, again, the
24 way that we organized these chapters was yet
25 again based on this network stack abstraction.

1 So chapter 5 and 6 were specifically
2 looking at the different layers of the network
3 stack, the top layer of which is the application
4 layer. And then one of the applications that
5 can exist at that layer is HTTP and HTTPS, which
6 are the protocols that you use for websites.

7 And so chapter 7 really is just diving in
8 on that, how do you protect websites, how do you
9 protect clients that connect to websites, how do
10 you connect servers from malicious clients.

11 MS. SHI: Well, thank you. Can we go off
12 record? I think we can take the break now, and
13 go off record.

14 (A recess was taken.)

15 Q. (By Ms. Shi) Let's just go over some
16 questions not really related to network technology.
17 So do -- you have reviewed the declaration of
18 Dr. Patrick McDaniel; is that right?

19 A. **Yes.**

20 Q. Do you know Mr. McDaniel in person?

21 A. **I know Dr. McDaniel in person, yes.**

22 Q. How do you know each other?

23 A. **We've met at computer security**
24 **conferences.**

25 Q. Do you know Jack Hobson, the inventor of

1 the '512 patent?

2 **A. Not personally. We may have had**
3 **interactions in the past, though, on other cases, as**
4 **I recall.**

5 Q. For the -- another case, are you talking
6 about the case -- cases we took deposition yesterday?

7 **A. No, unrelated cases.**

8 Q. Do you know any of the inventors of the
9 prior art references?

10 **A. Could you be more specific, please?**

11 Q. Sure. So Exhibit 1006 is a patent by
12 Kesanupalli. Am I saying it right?

13 **A. I don't know, because I don't know**
14 **Kesanupalli. So I would just say it, the way I just**
15 **said it.**

16 Q. Okay. And so you don't know the inventor,
17 Kesanupalli?

18 **A. I'm not personally -- met him, but I am**
19 **familiar with his work, his achievements, his**
20 **reputation. I speak to that in my declaration.**

21 Q. And Exhibit 1007 is a patent by Challenger.
22 Do you see that?

23 **A. Yes.**

24 Q. Do you know Challenger, personally?

25 **A. I do not know David Challenger personally,**

1 **but I also know of his work, his reputation. And I**
2 **speak of that in my declarations.**

3 Q. Exhibit 1008 is by Cheng, C-H-E-N-G. Do
4 you know Mr. or Mrs. Cheng?

5 A. **I don't know David Cheng. That does not**
6 **ring a bell, as I sit here today.**

7 Q. We have cited in the petition, additional
8 supporting references. Any of the author of those
9 supporting references, do you know them, personally?

10 A. **We'd already mentioned Patrick McDaniel.**
11 **I can't remember if he was an author of one of your**
12 **supporting references. And then there's a number of**
13 **other supporting references. I don't recall every**
14 **single one, but for example, there's a supporting**
15 **reference, Exhibit 1009, which is a patent to Brown,**
16 **et al. And I do not know, personally, any of the**
17 **authors of the Brown reference.**

18 Q. So let's talk a little bit about your
19 personal experience with defending against social
20 engineering attacks. Could you please describe any
21 real world social engineering attacks that you have
22 dealt with in your work?

23 A. **Sure. So going now to my CV. Yeah, so**
24 **there's a publication, one of my earliest**
25 **publications in the computer security area, which is**

1 listed in my CV as C-80, which is on a system
2 called -- we called TRICERT, T-R-I-C-E-R-T, all
3 capitals, which is getting at the issue of phishing
4 in e-mails.

5 So one of the ways that social engineering
6 occurs is that someone will send an e-mail to a
7 potential victim, where an attachment in that e-mail
8 is containing a computer virus, let's say. And they
9 try to trick, through whatever message is in the
10 e-mail, you know, we're the IRS or we're your
11 security company or your boss, whatever, click here
12 to find the important thing. And then people click.

13 This is called -- this is one of the ways
14 that phishing occurs. And I talk about that also in
15 my declarations. For example, in the paragraph that
16 talks about phishing attacks through e-mail.

17 And in this paper, we give a technique
18 that would prevent that through a certification
19 process, where only somebody who really is your boss
20 and now is certified to be your boss is sending you
21 this message. So it's something that presumably you
22 can trust as coming from your boss, rather than
23 somebody just pretending to be your boss, and trying
24 to get you to click it.

25 Q. So that's your research paper, right?

1 **A. Yes, dealing with the real world attack of**
2 **phishing through e-mails.**

3 **Q. Did you implement your technology in any**
4 **real world organizations or project?**

5 **A. I believe we did implement a prototype.**
6 **The student, D. Medarios, one of the coauthors on**
7 **that paper, my recollection is that he did do an**
8 **implementation prototype.**

9 **Q. Have you been involved in the education in**
10 **organizations or individuals to recognize and respond**
11 **to these types of attacks by social engineering?**

12 **A. Yes. So as we talked about earlier, I**
13 **have written a textbook on Introduction to Computer**
14 **Security. I've taught courses using that textbook**
15 **myself. And then I've been honored that this**
16 **textbook has been used at a number of other**
17 **universities to teach courses of how to protect**
18 **systems and people from all kinds of attacks,**
19 **including social engineering attacks, including**
20 **courses at Berkeley, University -- Brown University,**
21 **Virginia Tech University, and others.**

22 **Q. Any involvement other than the textbook?**

23 **A. Yes, I've also taught in -- here at UCI,**
24 **we have what we call a professional master's degree,**
25 **that is directed to professionals or future**

1 professionals in the computing sphere. And I've
2 taught my computer security course with similar kinds
3 of topics to either existing professionals or future
4 professionals in that course.

5 Q. So is it correct that a lot of your
6 research work is directed at cryptographic
7 technologies?

8 A. I have a number of papers that either
9 directly or indirectly utilize cryptographic
10 techniques.

11 Q. For computer security, could you provide
12 some examples of how crypto concepts can be used?

13 A. Sure. So the paper we just discussed was
14 C-80, TRICERT. That used cryptographic techniques to
15 do this certification, what we called certified
16 e-mail, where you could be assured that the e-mail
17 was from somebody who was trusted.

18 Another very influential paper that was a
19 part of a big -- over a million dollars grant from
20 DARPA is publication C-83. And this is the system
21 behind the prototype that we ultimately developed
22 through the company I talked about yesterday called
23 Algomagic, that was all about certifying the digital
24 certificates that are used in -- for example, as a
25 part of the HTTPS protocol.

1 So, for example, one of the ways you can
2 protect against phishing attacks is to verify that
3 when you use this HTTPS protocol, that you're going
4 to a website that has a valid digital certificate
5 that's used to encrypt that session.

6 And our system described here first in
7 C-83, and then we did a technology transfer to the
8 company. And, in fact, got an award -- technology
9 transfer award for, was for that technology. That
10 was a cryptographic technique. And I could go on. I
11 mean, there's dozens of other papers I could discuss
12 as well.

13 Q. Yeah, I think one thing is -- one
14 technique I read about security is called message
15 authentication codes. Does that -- is that familiar
16 tell you?

17 MR. FISHBACK: Objection, form, scope.

18 THE WITNESS: Yes, we talked about them
19 earlier today, if you recall. They're already
20 on the record for today.

21 Q. (By Ms. Shi) Is it related to digital
22 signature?

23 A. In some contexts, it could be thought of
24 as like a poor man's digital signature, because it
25 only works for the purpose of integrity if two

1 parties share a secret key.

2 And so it's not truly -- I mean, it's kind
3 of like -- it has some overlap with, like, a digital
4 signature, but it's not exactly that, because they
5 have to share the secret key in order to both produce
6 the MAC, the HMAC, as well as to verify a message
7 using an HMAC at the other end. They have to have a
8 key in order to achieve it.

9 Q. So is it fair to say that the message
10 authentication codes help to achieve the integrity
11 goal for security?

12 A. Yes, generally speaking, that's how they
13 are used today.

14 Q. So can message authentication codes be
15 used to protect sensitive files that are saved on a
16 computer?

17 A. I think that depends on the context, and
18 how they would be used.

19 Q. So is it correct that, in some contexts,
20 message authentication codes can be used to protect
21 sensitive files on a computer device?

22 MR. FISHBACK: Objection, form, scope.

23 THE WITNESS: It, again, depends what you
24 mean by protect. So if by protect, you mean to
25 achieve some level of integrity that the files

1 have not been changed, then there may be -- it
2 may be possible, in some cases, to come up with
3 a scheme based on hashed message authentication
4 codes to achieve that.

5 Q. (By Ms. Shi) And can message
6 authentication codes be used to -- for multiple
7 parties on the network to verify the integrity of a
8 file?

9 A. Yes, that's something that could be done
10 using message authentication codes, in some contexts.

11 Q. So what are some other techniques that are
12 used for file protection?

13 A. We talked about some of them already
14 today. So one we talked about was encryption.
15 Another we talked about was access rights and access
16 control. Another one is memory protections. And
17 another one we also talked about is encryption, if I
18 haven't mentioned that already. There's a number of
19 techniques that are in use today for that purpose.

20 Q. What do you mean by memory?

21 A. I mean memory for computers, so either the
22 main memory in RAM for a computer or it's external
23 drives.

24 Q. Sorry if I missed that, I don't recall we
25 talked about memory protections -- memory protection

1 techniques?

2 A. Okay. So this is now when I get to
3 pretend to be the professor scolding the student
4 during office hours, that we did talk about that.
5 Namely, we talked about virtual memory protection.

6 Q. Okay.

7 A. We talked about file system protection,
8 which is another form of memory. We talked about
9 process memory protections between multiple
10 processors. So we did talk about those as techniques
11 in use today that protect memory. Sorry to be the
12 scolding professor.

13 Q. Okay. So is the memory protection
14 different from file system protection?

15 MR. FISHBACK: Objection, form, scope.

16 THE WITNESS: So memory protection is
17 broader, because a file system is a specific
18 organization for memory into a file system. So
19 memory protection is a broader concept, the way
20 that we discussed it today with respect to
21 memory protection.

22 Q. (By Ms. Shi) So is memory protection the
23 same as data protection?

24 MR. FISHBACK: Objection, form, scope.

25 THE WITNESS: No, not the way that -- I

1 mean, of course, that depends on the context.
2 But data protection is yet another overlapping
3 concept of protecting the contents of data,
4 which could be in memory, so it definitely
5 overlaps.

6 But now moving it to another memory, you
7 still want to protect that same data. So it's
8 an overlapping concept. It's not identical.
9 It, again, depends on the context, but generally
10 speaking, that would be true.

11 Q. (By Ms. Shi) So are techniques protecting
12 data different from techniques protecting memory?

13 A. They overlap. So some techniques are used
14 for both, and then some might be used for one and not
15 the other.

16 Q. So we talked about authentication
17 techniques. Is that a technique that can be used for
18 both data protection and memory protection?

19 A. It could be a component in a system that
20 is being used for either or both, depending on the
21 context.

22 Q. We also talked about access control. Is
23 access control a technique that can be used to
24 protect both memory and data?

25 A. Yes, that's something that also is in use

1 **today for potentially protecting either or both.**

2 Q. We also talked about encryption. Is
3 encryption a technique that can be used to protect
4 both memory and data?

5 A. **Yes, that's also a technique that I**
6 **believe is in use today for protecting either or**
7 **both.**

8 Q. So what are some techniques that only
9 protect data, but are not applicable to protection of
10 memory?

11 MR. FISHBACK: Objection, form, scope.

12 THE WITNESS: So nothing specific is
13 coming to mind, but it could depend, for
14 example, on how you use those other techniques,
15 the specific ways that you're doing the, say,
16 encryption versus how you're using it with
17 memory or for data.

18 Q. (By Ms. Shi) Are there techniques that
19 only apply to memory protection, but not applicable
20 to data protection?

21 MR. FISHBACK: Objection, form, scope.

22 THE WITNESS: Yeah, I would need more time
23 to think about that. Nothing is specifically
24 coming to mind, but there may be some things.

25 MS. SHI: Okay. I would like to take a

1 break, if that works for you.

2 THE WITNESS: Yeah, now we can take the
3 lunch break, and then be back in an hour.

4 MS. SHI: Okay, that will work. So we
5 will be back here at my 3:20.

6 THE WITNESS: Sounds good.

7 MR. FISHBACK: Ms. Shi, just for my own
8 planning purposes, do you know how long you plan
9 on taking today? And if you don't, that's
10 completely fine, but I'm just trying to plan out
11 something after 5:00 today, so --

12 MS. SHI: Yeah, 5:00 Central, right?

13 MR. FISHBACK: Yeah.

14 MS. SHI: I expect to wrap up definitely
15 before 5:00.

16 MR. FISHBACK: Awesome. Thank you.

17 THE WITNESS: All right. See you guys at
18 3:20 your time.

19 MS. SHI: Thank you.

20 (A luncheon recess was taken.)

21 Q. (By Ms. Shi) So we have taken multiple
22 breaks today. Have you spoken with anyone during
23 those breaks?

24 A. Not about anything to do with my
25 testimony.

1 Q. Did you review any documents during the
2 breaks?

3 A. **Not that I recall.**

4 Q. Did you communicate with anyone about this
5 deposition today?

6 A. **No.**

7 Q. So at the beginning of this deposition,
8 you had your e-mail application open and used that
9 e-mail application to send Exhibit 1; is that right?

10 A. **Yes.**

11 Q. After you closed that e-mail application,
12 did you use any other applications, other than PDF
13 and the finder tool?

14 A. **Not on this computer.**

15 Q. Did you consult any documents other than
16 Exhibit 1 on your computer today?

17 A. **I consulted other exhibits that we
18 discussed today on my computer, including
19 exhibit -- not during breaks, but during the time on
20 the record that we discussed. So all the exhibits we
21 discussed on the record, I consulted on my computer.**

22 Q. Did you consult any other documents on
23 your computer today?

24 A. **Not that I recall.**

25 Q. Did you consult any other documents not on

1 your computer today?

2 A. No.

3 MS. SHI: I don't have additional
4 questions. I pass the witness.

5 MR. FISHBACK: Nothing further from me.
6 Thank you, Dr. Goodrich.

7 (Whereupon, at 4:24 p.m., the deposition
8 concluded.)
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 E R R A T A S H E E T

2 Pursuant to Rule 30(e) of the Federal
3 Rules of Civil Procedure and/or Official Code of
4 Georgia Annotated 9-11-30(e), any changes in form or
5 substance which you desire to make to your deposition
6 testimony shall be entered upon the deposition with a
7 statement of the reasons given for making them.

8 To assist you in making any such
9 corrections, please use the form below. If
10 supplemental or additional pages are necessary,
11 please furnish same and attach them to this errata
12 sheet.

13 * * *

14 I, the undersigned, MICHAEL T. GOODRICH,
15 Ph.D., do hereby certify that I have read the
16 foregoing deposition, and that to the best of my
17 knowledge, said deposition is true and accurate (with
18 the exception of the following corrections listed
19 below).

20 Page____Line____should read:_____

21 Reason for change:_____

22 Page____Line____should read:_____

23 Reason for change:_____

24 Page____Line____should read:_____

25 Reason for change:_____

1 Page____Line____should read:_____

2 Reason for change:_____

3 Page____Line____should read:_____

4 Reason for change:_____

5 Page____Line____should read:_____

6 Reason for change:_____

7 Page____Line____should read:_____

8 Reason for change:_____

9 Page____Line____should read:_____

10 Reason for change:_____

11 Page____Line____should read:_____

12 Reason for change:_____

13 Page____Line____should read:_____

14 Reason for change:_____

15

16

17 _____

Signature

18

19

20 _____, Notary Public.

21 This, the_____day of_____, 2025.

22 My Commission Expires:_____.

23

24

25

26

27

D I S C L O S U R E

STATE OF GEORGIA) DEPOSITION OF
HENRY COUNTY) MICHAEL T. GOODRICH, PH.D.

Pursuant to Article 10.B of the Rules and Regulations of the Board of Court Reporting of the Judicial Council of Georgia, I make the following disclosure:

I am a Georgia Certified Court Reporter. I am here as a representative of Henderson Legal Services, Inc.

Henderson Legal Services, Inc. was contacted by the offices of Haynes and Boone, LLP to provide court reporting services for this deposition. Henderson Legal Services, Inc. will not be taking this deposition under any contract that is prohibited by O.C.G.A. 9-11-28 (c).

Henderson Legal Services, Inc. has no contract or agreement to provide court reporting services with any party to the case, or any reporter or reporting agency from whom a referral might have been made to cover the deposition.

Henderson Legal Services, Inc. will charge its usual and customary rates to all parties in the case, and a financial discount will not be given to any party in this litigation.


F. Renee Finkley, RPR, CRR, CLR
Georgia CCR-B-2289

Henderson Legal Services

202-220-4158

www.hendersonlegalservices.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

C E R T I F I C A T E

STATE OF GEORGIA:
COUNTY OF HENRY:

I, F. Renee Finkley, a Certified Court
Reporter in and for the State of Georgia, do hereby
Certify:

That prior to being examined, the witness
named in the foregoing deposition was by me duly
sworn to testify to the truth, the whole truth, and
nothing but the truth.

That said deposition was taken before me
at the time and place set forth and was taken down by
me in shorthand and thereafter reduced to
computerized transcription under my direction and
supervision, and I hereby certify the foregoing
deposition is a full, true and correct transcript of
my shorthand notes so taken.

I further certify that I am not of kin or
counsel to the parties in the case, and I am not in
the regular employ of counsel for any of the said
parties, nor am I in any way financially interested
in the result of said case.

IN WITNESS WHEREOF, I have hereunto
subscribed my name this 8th day of January, 2025.



F. Renee Finkley, RPR, CRR, CLR
Georgia CCR-B-2289

A				
AAA 38:6	68:19	72:23	anymore 36:22	asking 19:24
able 16:10	achieving	algorithmics	API 35:16	20:25 26:22
18:1 28:4	44:18 58:9	12:9	36:18,24	27:17 32:5
39:24 43:9	62:10	algorithms	37:2,9	32:24 33:4
47:9 60:4,7	acknowledge	11:1,7,11,12	apologize 57:1	35:8
abstraction	22:10	11:14,15,16	APPEAL 1:3	aspect 21:15
50:6 66:25	Acrobat 18:25	11:16,17,17	appear 17:6	assigned 53:4
accept 31:15	actions 17:8	11:18,24,25	26:3	assist 82:8
31:19,22	actively 53:11	11:25 12:1,1	APPEARAN...	associated
32:14,20	actual 44:12	12:8,25 13:4	2:1	31:16 33:11
33:10 66:1	50:12 57:9	13:8,11,19	Apple 1:6 4:8	48:20
acceptance	addition 6:9	Alice 32:1	60:14	assurance
32:8	12:6 17:4	39:20 42:4	applicable	38:7,24
accepted 32:2	18:6 19:14	42:12	78:9,19	assured 72:16
accepting	22:14	Alice's 30:9,19	application	attach 82:11
65:23,25	additional	31:5,23	14:11 19:2	attached 35:24
accepts 52:11	38:6 39:11	alleged 7:18	67:3 80:8,9	35:25
access 14:3	69:7 81:3	9:16	80:11	attachment
35:13 36:8	82:10	allocated	applications	70:7
36:15 39:5,6	address 17:1	51:24	11:15 14:8	attachments
44:15,20	50:4 51:8	allow 49:20	17:24 18:11	22:4
45:10 48:2	addressing	allowed 15:19	18:14,23	attack 26:8
48:24 49:17	45:6	altered 41:13	24:11 65:1	43:22,23
50:3 51:1	administrator	41:16	67:4 80:12	46:13 51:21
53:3,8 60:1	53:5	Amazon 15:15	applied 22:9	51:22 52:7
60:24 61:1,7	administrato...	analysis 11:16	applies 5:20	52:10 55:7,8
61:13 75:15	48:5	and/or 27:2	apply 5:23	55:18 65:17
75:15 77:22	Adobe 18:25	82:3	78:19	65:19,20
77:23	advanced	Annotated	architecture	66:3 71:1
accessible	11:23 13:21	82:4	34:1,9,16	attacker 45:9
48:22	advocating	anonymity	area 35:14	45:10 46:22
account 31:16	24:16 26:9	38:7,25	36:16 69:25	52:5,8 66:2
33:11	afield 50:1	answer 4:16	arguments	attackers
accountant	agency 84:15	4:18 5:11	6:24 7:1,15	63:13
53:5	ago 18:4	19:19 20:1,6	art 7:17,18 8:9	attacking
accurate 4:22	agree 27:13	20:10,15,24	9:16 22:24	64:14,18
82:17	54:8	21:1 28:4	27:21,24	65:5,14,21
achieve 40:14	agreement	36:10	31:20 33:25	attacks 21:24
48:1 50:6	84:14	answered 20:9	35:3 68:9	24:25 25:3
53:2,9 65:6	agreements	anticipate 5:3	Article 84:5	25:15,21
74:8,10,25	15:20	anticipation	asked 5:11	26:1,5,12,25
75:4	akin 59:16	9:22	18:3,4 21:4,5	27:4,12,16
achievements	al 69:16	antivirus	28:3 32:16	27:18 28:1
	Algomagic	56:17 57:19	47:13	43:21,25

44:3 45:13 45:14,19 46:10,20 47:4 48:7 49:4 50:20 51:18,19,19 52:16,18,19 52:20,25 53:21,22 54:5,6 64:12 64:14,16,16 65:4,5,7,10 65:13 69:20 69:21 70:16 71:11,18,19 73:2 Austin 2:11,20 authenticate 24:2 authenticating 40:11 authentication 24:3 28:21 28:23 29:5,8 29:9,12,18 29:22 30:11 30:16 40:4,7 40:17 73:15 74:10,14,20 75:3,6,10 77:16 authenticator 28:24 authenticity 38:7,25 40:15 55:13 author 69:8,11 authorization 55:13 authorized 44:16 49:21 51:2 authors 69:17 automatically	31:18 33:12 availability 38:3,14,22 43:5,6,10,11 43:19,20,23 44:1,21,22 available 15:15 43:7 43:17 59:23 60:10 award 73:8,9 aware 9:17 22:21 26:13 61:10 awareness 22:15 Awesome 54:15 79:16 B B-O-T-S 55:6 back 20:15 60:25 63:20 63:21 79:3,5 backed 31:23 background 27:5 backup 31:22 31:25 32:9 37:14,14 backups 31:15 31:19 32:15 32:20 33:10 bad 53:12 bank 29:16 34:4 based 15:19 64:22 66:25 75:3 began 12:14 12:19 beginning 11:3 27:6 29:3,20 30:8	31:13 33:8 35:10,20 80:7 begins 23:16 35:12 behalf 2:3,16 4:8 believe 7:7 11:8 15:2,15 19:1,3 71:5 78:6 bell 69:6 benefit 43:25 Berkeley 71:20 best 5:13 20:1 20:4 22:3 82:16 beyond 52:13 big 72:19 bigger 52:6 binary 57:9 binding 25:13 BIOMETRICS 1:9 bit 69:18 bits 57:9 board 1:3 6:14 84:6 Bob 39:16,21 40:1 42:1,5 42:13 58:22 58:24 59:2,6 book 13:20 15:4 37:18 38:5 44:9,9 61:19 Boone 2:8 4:8 84:10 boss 70:11,19 70:20,22,23 bots 55:5 bottom 64:25 Boulevard 2:9	break 5:15 26:1 28:7 46:19,21 47:1 48:8 53:11 54:12 54:14,18 67:12 79:1,3 breaking 21:19 60:5 breaks 5:14 79:22,23 80:2,19 broad 64:8 broader 76:17 76:19 broadly 66:20 brought 50:11 Brown 69:15 69:17 71:20 browser 19:5 19:7 buffer 51:18 51:22,22,25 52:5,6,7,10 52:13 build 45:6 47:8 48:6 built 26:11 C c 84:1,12 85:1 85:1 C-80 70:1 72:14 C-83 72:20 73:7 C-H-E-N-G 69:3 California 5:4 11:5 call 6:7 39:16 39:19,24 42:1 55:5 57:14 71:24	called 12:24 13:17 14:1 42:10 50:7 55:25 56:25 62:19 70:2,2 70:13 72:15 72:22 73:14 camera 29:16 36:2 capitals 70:3 CARBYNE 1:9 card 45:9,10 45:21,21,25 careful 32:6 case 6:15,23 24:15 30:15 30:23 39:14 42:13 68:5,6 84:14,17 85:12,13 cases 5:17 6:23 62:9 65:24 68:3,6 68:7 75:2 catch 64:1 caught 46:2 cause 13:23 60:20 CCR-B-2289 1:25 84:22 85:20 center 45:11 centers 44:14 Central 79:12 certain 49:16 57:8,8,10,11 57:14 65:25 certificate 73:4 certificates 72:24 certification 70:18 72:15 certified 70:20
--	---	--	---	---

72:15 84:8 85:4 certify 82:15 85:5,10,11 certifying 72:23 Challener 68:21,24,25 chance 54:11 change 10:19 44:25 82:21 82:23,25 83:2,4,6,8,10 83:12,14 changed 75:1 changes 14:17 82:4 chapter 15:3 44:10 45:4 47:7 52:17 54:19 61:16 61:16 62:17 66:14 67:1,7 chapters 13:20,25 65:3,11 66:24 characterize 64:20 charge 84:16 chat 16:10 check 56:11 58:8 63:19 checking 57:1 57:23 Cheng 69:3,4 69:5 chunks 50:9 CIA 38:2 cipher 39:24 circumvents 21:16 cited 69:7 Civil 82:3	claim 32:4,6 32:25 33:2,5 34:5,11 37:11,12 claims 26:22 27:20,23 clarification 17:19 clarify 33:5 class 13:15,24 14:21,22 15:1 17:2 19:16 21:22 37:15 classes 12:11 12:16,17,21 12:23 13:9 13:10 classmen 13:7 clear 5:18,24 click 22:5 55:1 56:3 70:11 70:12,24 client 29:23 clients 60:21 67:9,10 close 18:10 19:11 28:5 closed 18:12 80:11 closely 66:7 closing 19:13 cloud 29:17,25 30:6,7,10,13 30:24 31:14 31:24 32:2 32:14,19 33:9 34:15 64:17 CLR 1:24 84:22 85:19 coauthored 12:7 13:16 14:2	coauthors 71:6 code 57:23 82:3 codes 73:15 74:10,14,20 75:4,6,10 coercion 45:23 coincide 13:25 colleagues 57:2 Colorado 2:19 column 27:6 29:3,19 30:8 31:14 33:6 35:10,12,21 36:15 37:10 combination 47:11 come 49:8 53:22 75:2 comfortable 7:24 coming 26:16 27:19 41:9 43:2 49:5 55:17 70:22 78:13,24 commercially 60:9 Commission 83:20 common 56:21 58:13 62:16 commonly 56:18 communicate 18:5 29:14 30:7,10 35:15 36:3,6 36:17,21,25 37:13 63:8	64:4 80:4 communicat... 30:3 64:15 communicat... 29:14 communicat... 18:14 35:6 36:24 63:1 65:8 communicat... 51:24 62:1 65:9 company 53:10 58:4 60:14 70:11 72:22 73:8 compare 42:23 complete 4:22 completely 4:16,19 49:9 51:14 79:10 component 77:19 components 34:15 40:13 compromise 44:24 45:1 computational 11:12 computation... 41:4 compute 41:2 42:22 computer 3:9 9:21 11:2,11 11:12,23 12:4,6,7,21 12:24 13:4,8 13:10,13,15 13:17,18 14:1,12,14 14:18 15:1 15:13 17:1	17:25 18:15 18:24 21:16 21:19,21 22:9 25:20 27:22,25 29:7 37:15 37:24 38:4,8 38:10 47:17 48:14,15 50:1,12 51:4 51:9 52:9 53:1,2 54:22 54:24,24 55:2,12,15 55:25 56:15 56:24 57:14 58:12,14 59:18,24 60:1,3 61:21 62:22 63:13 63:19,25 65:13,22,23 66:3 67:23 69:25 70:8 71:13 72:2 72:11 74:16 74:21 75:22 80:14,16,18 80:21,23 81:1 computerized 85:9 computers 44:20 54:25 55:4,7 61:24 62:2,4 63:14 75:21 computing 11:23 44:13 72:1 concatenate 42:16,22 concept 17:4 21:7 37:24
---	--	---	---	--

38:11 39:2 40:15 76:19 77:3,8 concepts 14:4 16:25 37:24 38:3,4,8 72:12 concerning 11:1,7 12:4 concerns 11:21 concluded 81:8 conclusions 7:19 conferences 67:24 confidential 21:9,13 39:4 39:20 40:13 41:14 confidentiality 38:2,13,21 39:1,2,12 40:5,8,10,19 40:21 41:7 44:6,24 configuration 30:18 configured 31:15 32:14 33:10 confirm 18:22 19:4,7 confused 20:1 conjunction 40:8 connect 29:24 43:8 66:11 67:9,10 connected 47:19 61:24 connecting 34:4	connection 36:10 46:4 connections 34:2 65:24 65:25 66:2 66:20 considered 24:21 consult 15:7 20:7 80:15 80:22,25 consulted 80:17,21 contacted 84:10 containing 70:8 content 64:15 contents 3:1,8 15:22 16:5 19:21 20:3 37:17,22 44:8 48:11 49:18,20 61:19 63:2 77:3 context 24:7,9 24:11,12,20 48:16 74:17 77:1,9,21 contexts 21:8 73:23 74:19 75:10 continues 52:12 continuing 11:4 35:11 contract 84:12 84:13 control 14:3 48:3 60:24 61:1 75:16 77:22,23 controls 44:15	61:13 copies 43:14 copy 15:16 copyright 15:15,19 16:6 correct 9:19 10:15 14:12 17:20,23,25 19:6 24:18 25:19,24 27:8 29:18 30:23 34:8 35:17 38:12 46:23 53:24 55:16 57:18 60:25 62:6 66:6,21 72:5 74:19 85:10 corrections 82:9,18 Council 84:6 counsel 2:1 7:19 9:3 18:6 85:12,12 COUNTY 84:3 85:2 course 12:24 13:13,18 14:13,18 27:20 36:19 38:10 47:12 51:14 72:2,4 77:1 courses 11:1,6 11:9,20,21 11:22 12:3,5 12:13,14,18 71:14,17,20 court 9:13,18 15:25 16:14 20:14,16 84:6,8,10,14 85:4	cover 13:14 14:25 16:6 17:12,13 84:15 created 41:12 credentials 17:9 25:13 25:16 27:3 55:16,19 Cross-talking 20:12 CRR 1:24 84:22 85:19 crucial 21:15 crypto 72:12 cryptographic 14:4 21:16 21:19 39:9 40:21 41:4 42:15,17 72:6,9,14 73:10 cryptography 14:9 39:14 59:2 cues 21:7 customary 84:17 CV 11:9 69:23 70:1 cyber 11:13,24 12:8	33:18,19,22 39:3,5,8 40:2 40:22 41:12 42:2 43:6 44:14,25 45:10 51:1 61:6,7,9,11 62:5,24 63:3 63:5,9,23 64:3,4,7,8 76:23 77:2,3 77:7,12,18 77:24 78:4,9 78:17,20 date 14:13 David 2:6 68:25 69:5 david.obrien... 2:14 day 83:20 85:14 deal 38:6 53:1 dealing 50:24 71:1 dealt 69:22 decision 6:14 8:8 declaration 5:22 6:6,12 7:3 8:6 10:2 10:6,9,12,14 10:21 19:9 23:12,15,22 24:17 25:25 47:13 49:10 50:1 51:15 67:17 68:20 declarations 5:21 6:1,5,11 6:17 7:13,21 8:6,7 9:21 22:23 69:2 70:15 decrypt 40:2
--	--	--	--	---

58:25 59:4 59:12 60:6 63:18 decryption 14:10 dedicated 35:15,17 36:1,17 defend 21:23 22:16 23:3,9 24:5,12,19 24:24 25:2 26:14,19 27:11 45:2 45:12 49:4 50:21 53:13 defending 22:22 44:2 52:9 69:19 define 37:16 definitely 77:4 79:14 degree 71:24 denial 43:21 43:24 55:7 65:6 depend 78:13 depending 54:9 77:20 depends 24:7 24:9,11,20 32:3 74:17 74:23 77:1,9 deposition 1:17,22 4:12 5:1,8 8:1,18 9:6,8,10 20:5 28:6 37:19 44:8 61:20 68:6 80:5,7 81:7 82:5,6 82:16,17 84:2,11,12 84:15 85:6,8	85:10 depositions 8:23 describe 11:6 28:18 69:20 described 23:3,9 26:18 27:9,15 29:4 33:14 52:19 64:16 73:6 describes 26:25 design 11:2,16 13:6 designed 64:24 designer 56:7 desirable 46:8 46:19,21,25 47:20 48:21 54:4 desire 82:5 detail 14:24 29:5 details 22:1 detection 11:13,24 12:8 determine 39:25 40:16 developed 72:21 developer 58:4 development 53:18 developments 14:14 device 28:24 29:14 30:6 30:21 31:8 33:9 34:21 34:25 35:1 35:21 47:10	56:18 57:19 57:24 61:2 74:21 devices 29:10 29:15,23 30:21 31:7 31:16,17 32:20 33:10 33:12 34:14 44:13 47:19 64:18 65:14 66:19 diagram 33:19 34:16 diagrams 33:22 dictionary 26:1,4,5,8 different 41:14 53:9 57:2,15 60:25 67:2 76:14 77:12 difficult 25:7 41:5 45:18 46:9,13,16 47:1,8 digital 41:23 42:3 55:20 56:12 57:3 57:16,23 58:3,8,20 59:5,15,17 72:23 73:4 73:21,24 74:3 digitally 42:1 56:8,9 58:4 diligent 22:13 directed 13:3 64:17 66:20 71:25 72:6 direction 41:2 85:9 directly 36:4,6	72:9 disagree 32:19 disassemble 44:20 disclose 15:9 disclosed 28:21 31:2,4 discloses 25:8 disclosing 15:8 37:12 disclosure 84:7 disclosures 35:12 discount 84:17 discovered 60:19 discuss 19:15 21:22 22:23 37:21,23 62:17 73:11 discussed 13:25 30:5 35:10 38:24 47:13 48:12 58:16 60:24 72:13 76:20 80:18,20,21 discussing 5:17 51:20 discussion 16:20 20:18 23:16 46:6 46:17 57:21 discussions 7:18 11:10 23:20 disguises 21:11 dispute 33:1 distributed 58:15 District 9:13	9:18 divided 50:9 diving 67:7 documents 6:2,9,10,15 6:23 8:2,4 9:2,6,12,18 19:1,8 80:1 80:15,22,25 doing 17:7 21:17 36:22 36:23 42:5 56:25 63:16 63:24 78:15 dollars 72:19 download 21:14 43:8 downloading 17:9 dozens 73:11 Dr 6:13 8:7 16:5,12 17:22 20:17 20:19,23 67:18,21 81:6 draft 8:12 drive 19:3 50:14 51:6 60:15,22 drives 75:23 duly 4:3 85:6
E				
E 82:1,1,1 84:1 85:1,1 e-mail 7:3 8:17 16:13,13 17:24 18:2,3 18:4,11,20 22:4 55:1 70:6,7,10,16 72:16,16 80:8,9,11				

e-mails 56:2 70:4 71:2	encrypted 58:17 59:11 59:13 60:3 60:15 62:24 62:24 63:9 63:15 64:3,7	entities 36:21 37:1 51:25	72:24 73:1 78:14	17:17
e.g 36:1	59:13 60:3	entity 39:16 42:1	examples 21:10 29:23 49:5 60:12 61:15 72:12	face 46:1
earlier 13:16 17:23 36:14 41:25 57:17 58:2,2,21 71:12 73:19	encrypting 63:22	environment 28:20 29:7 29:21	exception 82:18	fact 50:4 56:8 59:16 60:18 73:8
earliest 69:24	encryption 14:9 58:16 58:18,21,22 59:18 60:5 61:12,13 62:7,9,15 63:6 75:14 75:17 78:2,3 78:16	errata 82:11	exhibit 3:7 10:3 15:16 16:1,2 18:6 18:19 19:23 37:19 44:7 61:19 68:11 68:21 69:3 69:15 80:9 80:16,19	factors 45:5 fair 5:12 74:9 familiar 68:19 73:15
early 12:19,23 13:5		error 10:14	exists 34:2 49:7 64:9 67:5	far 49:25
easier 16:17		especially 53:14	existing 72:3	fast 35:14,24 37:6
easy 41:1		Esq 2:5,6,7,17	exhibits 3:6 19:1,3 80:17 80:20	Federal 82:2
eavesdrop 62:25		establish 36:9	exist 34:2 49:7 64:9 67:5	fight 55:21 58:18
eavesdroppi... 65:9		estimate 7:23	exists 64:1 66:4	figure 28:16 28:18,19 29:15,20 33:15,17,21 33:21,22,24 34:9,13,18 34:19,20 35:1,2,7,9,22
educating 25:5	et 69:16	everybody 39:22 59:4	expect 79:14	file 15:17 18:2 47:19 49:11 49:14 75:8 75:12 76:7 76:14,17,18
education 71:9	encrypts 62:21	evidence 42:25 56:13	experience 69:19	filed 9:12
either 7:3 60:4 72:3,8 75:21 77:20 78:1,6	enforce 48:10	exactly 14:21 37:4 74:4	Expires 83:20	files 49:16,18 49:20 59:19 59:23 60:3 60:15 74:15 74:21,25
embodied 39:6	engineering 14:25 17:1,3 19:15 21:5,7 21:15,23 22:12,17,22 23:1,4,10 24:5,13,19 24:25 25:2 25:15,21 26:6,12,14 26:20 27:1 27:11,16,18 28:1 44:2 45:3,5,8,14 45:18,24 46:9,20 47:4 49:4 69:20 69:21 70:5 71:11,19	EXAMINATI... 3:3 4:5	explain 13:22 24:8 25:1	financial 84:17
embodiment 28:20 29:21 31:3 34:21 34:25 35:9		examined 4:3 85:6	explained 24:16	financially 85:13
embodiments 31:12,14 32:24,25 33:1,9		example 6:6 9:15,16 21:12 23:12 23:15 27:5 29:7 30:19 33:21 34:3 34:17 35:10 35:21,22 37:13 39:7,9 41:18,20,22 42:12 44:13 45:20,20 47:23 48:1,5 48:19,25 49:16 55:11 55:14,24 60:13 63:6 65:12 66:5 69:14 70:15	explains 29:4 explicit 48:23 external 15:7 36:8,10 50:14 51:6 51:11 75:22	find 19:2 41:5 70:12
emergency 5:6	entered 82:6		F	finder 19:2 80:13
employ 85:12	enterprise 53:6,16		F 1:24 84:22 85:1,4,19	fine 28:8,9 79:10
employer 30:19,20,22 30:24 31:6,6 31:9	entire 6:23 50:3		F-I-S-H-I-N-G	fingerprint
encrypt 39:21 58:24 59:3,8 59:10,23 63:7 73:5	entirety 10:11			

25:9 36:2 Finkley 1:24 84:22 85:4 85:19 fire 5:7 fires 5:4 firms 60:19,20 first 4:3 10:23 12:17,20 23:22 31:10 32:4 33:7 34:6,10,16 34:22,23 38:1 48:23 56:11 63:7 65:18 73:6 Fishback 2:17 7:7 8:20 16:12,17,22 16:23 17:15 18:18 19:17 20:21 21:25 22:18 23:5 24:6 28:8 29:1 31:1 32:22 33:16 34:12 36:5 37:3 38:15 40:6 44:4 46:3 47:2,5 49:24 50:23 54:7,10,15 55:10 56:20 57:25 59:20 61:3,22 62:13 63:10 64:19 65:15 66:9,22 73:17 74:22 76:15,24 78:11,21 79:7,13,16 81:5 flash 60:22	flow 33:18,19 33:22,23 flowchart 33:18,23 focus 5:10 focused 33:5 following 14:15 82:18 84:6 follows 4:4 foregoing 82:16 85:6 85:10 form 19:17 21:25 22:18 23:5 24:6 29:1 31:1 32:22 33:16 34:12 36:5 37:3 38:15 40:6 44:4 47:2 49:24 54:7 55:10 56:20 57:25 59:5,15,20 61:3,22 62:13 63:10 64:19 65:15 66:9,22 73:17 74:22 76:8,15,24 78:11,21 82:4,9 forth 85:8 forward 5:1 16:24 fraud 11:13,24 12:8 freshmen 13:6 front 28:14 full 85:10 fun 51:13 function 40:23 41:1,4 42:15	42:18,23 functionality 43:16 functions 40:21 fundamental 37:24 fundamentals 11:14 furnish 82:11 further 81:5 85:11 future 71:25 72:3 G gain 45:10 60:1 garbage 60:6 general 22:8 43:17 generally 17:3 21:6 24:21 25:23 27:22 47:20 48:21 54:8 61:4,23 64:6 74:12 77:9 geometry 11:12 GEORGE 2:17 Georgia 82:4 84:2,6,8,22 85:2,4,20 getting 61:9 70:3 gfishback@... 2:22 give 24:14 25:23 50:2 52:5 60:12 65:12 70:17 given 41:3 82:7 84:17	gives 48:23 giving 45:9 52:8 go 4:10 5:1,14 10:2,5,20 23:21 25:10 28:16 29:2 29:19 30:8 37:1,17,20 38:1,6 44:16 54:16 57:14 62:17 66:12 67:11,13,15 73:10 goal 13:5 74:11 goals 38:13,19 38:22,24 44:3,18 53:3 62:10 goes 5:21 23:17,18 30:17 36:19 43:15 going 13:23 27:7 49:25 54:10 62:18 65:1 69:23 73:3 good 4:7,9,10 5:6 54:11 57:4 79:6 Goodrich 1:17 3:2 4:2 15:13 16:5,12 17:22 20:19 20:23 81:6 82:14 84:3 Goodrich's 20:17 graduate 10:25 11:3 grant 72:19 graph 11:14	11:25 graphical 52:2 graphics 11:13 great 16:7 ground 4:11 guard 26:25 27:15 46:1 guys 79:17 H H 82:1 hacker 41:17 handed 45:23 hang 18:19 happen 52:4 happy 32:12 hard 19:3 25:7 41:1,2 60:15 hardware 64:25 hash 40:21,22 41:4 42:15 42:17,23,24 hashed 75:3 Haynes 2:8 4:8 84:10 held 1:22 help 25:9 26:25 45:2 53:18 74:10 helps 44:3,5 Henderson 84:8,10,11 84:13,16 HENRY 84:3 85:2 hereunto 85:14 hiding 63:25 high 25:4 higher 14:7 25:23 highlighted
--	---	---	---	--

hijack 65:8	49:5	infect 54:25	interact 37:8	issue 49:15
HMAC 42:10	implement	55:4	interactions	52:14,25
42:11,20	71:3,5	influential	68:3	70:3
74:6,7	implementat...	72:18	interested	issued 30:22
Hobson 67:25	14:4 71:8	information	85:13	31:8
Hong 2:5 4:7	implemented	21:9,13	interface 52:2	issues 14:5
hong.shi@h...	33:15 35:1	30:12,16	internal 51:9	46:4 50:25
2:13	implementing	41:14,15	Internet 11:16	53:12
honored 71:15	39:11	initial 16:7	11:25 12:9	
Hopkins 11:5	important	initials 38:1	19:5 32:1,21	J
hour 28:5	44:17 61:21	injects 56:1	36:4,7,9	Jacinto 2:9
54:11 79:3	70:12	input 41:5	65:14	Jack 67:25
hours 7:20 9:1	importantly	42:17 52:1,5	interrupt 17:16	January 1:19
51:12 76:4	25:12	52:8	18:9 46:3	85:14
HTTP 67:5	impression	inputs 51:24	intervention	Jarrett 7:6
HTTPS 62:19	50:2	insecure 17:7	54:23	8:19
63:8,15,20	improve 25:20	21:18 35:24	introduce 38:5	Johns 11:5
63:22 67:5	improved	inside 51:4,9	44:25 47:21	joint 8:23
72:25 73:3	27:22,25	53:10 56:5	53:12,19	Judicial 84:6
human 22:14	55:12 63:5	63:17,22	introducing	
45:4 54:23	include 11:10	insider 52:18	41:17 63:13	K
	11:11,22	52:25 53:10	introduction	Kamprath 7:5
I	12:5,7 16:6	53:21,23	3:8 11:15	keep 14:12
ID 25:10	20:2 21:10	54:5	13:17 14:1	30:11
idea 41:23	29:11,11	insiders 53:16	15:12 37:20	keeping 30:15
56:24	34:9 41:23	53:25 54:1,3	44:9 71:13	44:14
identical 77:8	43:11 58:11	install 56:4,10	intrusion 66:3	KELLY 2:7
identification	included 12:18	58:7	invalid 55:19	kept 39:3,4
16:3	14:3	installation	inventor 67:25	Kesanupalli
identity 24:2	includes 15:22	56:11	68:16	22:24 23:9
39:25	22:24 29:8	installed 57:19	inventors 68:8	24:1,15,15
illustrate 34:3	35:23	installing	invert 41:1,2	24:23 25:1,4
illustrated	including 14:8	58:11	involved 71:9	25:12 26:10
35:1,22	14:9 27:1	institute 6:14	involvement	68:12,14,17
illustrates	29:15 45:13	institution 8:8	71:22	key 16:25 39:7
29:20	71:19,19	integrity 38:2	IPR 5:18,18	39:10,14,15
illustrating	80:18	38:13,21	6:6,13,14	39:17,17,21
35:9	inclusive	41:10,11,19	10:3	40:2 41:24
illustration	23:19 30:2	41:21,23	IPR2024-003...	41:25 42:13
28:19 33:25	incorrect 18:1	42:7,25 43:1	1:12	42:16,21,22
34:14,20	increase 62:8	44:6 45:1	IPR2024-003...	45:9,10,21
immediately	indirectly 72:9	58:9 73:25	1:13	45:21,25
26:15 27:19	individuals	74:10,25	IRS 70:10	47:11 58:22
41:9 43:2	42:12 71:10	75:7	Irvine 11:5	58:22,25
				59:1,3,4,8,10

59:12 60:2 74:1,5,8 keys 59:2 kin 85:11 kind 50:20 51:19 55:1 74:2 kinds 17:7,10 21:11 53:6 66:17 71:18 72:2 know 5:6,7,15 5:23 14:24 15:18 22:6 56:21 57:4 59:24 60:2 63:23 67:20 67:21,22,25 68:8,13,13 68:16,24,25 69:1,4,5,9,16 70:10 79:8 knowing 47:10 56:4 knowledge 82:17 known 22:24 25:25 39:13 39:22 48:2 48:15 51:21 52:7 63:18 64:23 65:17 knows 39:17 42:20	large 35:23 52:9 late 12:23 latest 14:13 law 60:18,20 layer 64:25 65:2,4 67:3,4 67:5 layers 14:6,7 64:24 67:2 leakage 49:1 learn 63:2 lectures 11:11 legal 6:24 84:8 84:10,11,13 84:16 legitimate 17:6 21:12 22:4,5 22:7 25:17 let's 9:20 10:2 10:20 16:1 23:21 33:3 53:10 54:13 54:16 67:15 69:18 70:8 level 13:2 25:4 74:25 levels 25:23 61:1 light 7:17 likewise 59:12 limit 53:3 limited 13:10 27:11 line 27:7,7 29:3,20 30:8 30:17 31:13 33:6,8 35:11 35:13,20 36:14 49:8 82:20,22,24 83:1,3,5,7,9 83:11,13 lines 46:14	list 6:6,8 23:14 listed 6:9 51:18 64:12 70:1 82:18 literally 18:3 litigation 9:18 84:18 little 32:6 69:18 LLC 1:9 LLP 2:8 84:10 located 29:6 locked 44:14 locks 47:7,8 log 25:11 logging 55:14 55:16 logical 33:23 long 8:25 79:8 longer 24:16 24:18,21,24 25:2,5,6,10 25:19,22 26:10 look 25:17 35:19 57:10 looking 7:15 67:2 looks 39:23 lot 72:5 lower 14:6 lunch 79:3 luncheon 79:20 LYLE 2:7	53:19 56:1 67:10 malware 14:6 21:14 52:17 53:22 54:5 54:19 55:21 55:24 56:19 58:18 man's 73:24 manager 53:6 manages 47:18 marked 16:2 master's 71:24 match 42:24 46:1,2 matches 59:11 59:13 matching 11:19 12:2 12:10 materials 14:18 15:7 matter 51:16 McDaniel 6:13 8:7 67:18,20 67:21 69:10 McKool 2:18 7:6,6,7 mean 31:19,21 32:3 36:7 38:17 49:7 66:11 73:11 74:2,24,24 75:20,21 77:1 means 39:9 40:25 45:17 46:8,16,19 46:25 56:3 meant 34:3 mechanism 41:25 mechanisms	49:19 61:8 Medarios 71:6 medical 5:1 meet 7:2 8:16 meeting 9:3 memory 20:5 47:19 48:20 48:21,24 49:2,2,11,14 49:23 50:4,5 50:8,8,12,16 50:17,21 51:4,5,6,9,11 51:23 52:11 52:12,14,15 75:16,20,21 75:22,25,25 76:5,8,9,11 76:13,16,18 76:19,21,22 77:4,6,12,18 77:24 78:4 78:10,17,19 mentioned 9:3 13:16 21:6 34:5 39:10 46:7 69:10 75:18 message 39:20 42:4 42:14,16,19 42:21 58:24 70:9,21 73:14 74:6,9 74:14,20 75:3,5,10 messaging 18:14 met 7:5 8:19 67:23 68:18 methodology 7:15 Michael 1:17 3:2 4:2 15:13
---	---	--	--	--

84:3	29:11 50:14	19:17 20:21	57:11	51:22 52:7
Microsoft 56:7	53:1 54:25	21:25 22:18	online 29:16	52:10
56:10 58:6	78:22	23:5 24:6	open 13:2	overlap 9:15
million 72:19	needs 37:1	29:1 31:1	17:24 18:15	52:22 74:3
mind 26:16	46:15 50:13	32:22 33:16	18:24,25	77:13
27:19 41:9	network 14:6,7	34:12 36:5	19:5,9,10,21	overlapping
43:3 49:6	14:7,8 29:25	37:3 38:15	44:23 80:8	77:2,8
78:13,24	30:4 61:17	40:6 44:4	operating 14:5	overlaps 77:5
minor 10:17	61:20 62:2,4	47:2,5 49:24	47:15,17,20	overloading
minute 18:4	62:8,10 63:7	54:7 55:10	47:22,24	43:22
minutes 16:16	64:11,18,23	56:20 57:25	48:1,4,7,9,16	overwrites
16:19	66:6,13,19	59:20 61:3	48:18 49:3	52:11
missed 75:24	66:20,25	61:22 62:13	49:19 51:23	overwriting
mobile 35:23	67:2,16 75:7	63:10 64:19	52:3 61:7	52:12
models 14:10	networking	65:15 66:9	operations	Owner 1:10
modified 48:4	11:2,21,22	66:22 73:17	61:25	2:16 7:8 8:10
modify 49:21	12:16,17,18	74:22 76:15	opine 28:3	8:13
60:4	29:16	76:24 78:11	47:14	Owner's 6:18
module 28:24	networks	78:21	opinion 10:17	
28:25 29:8	29:24 61:24	objections	opposite 45:6	P
modules 29:12	64:24	50:23	order 66:11	P-H 17:16
Monday 8:22	new 14:18	occur 62:3	74:5,8	P-H-I-S-H
morning 4:7,9	44:25	65:4	ordinary 7:17	21:10
4:10	Notary 83:19	occurs 70:6,14	27:21,24	p.m 1:20 81:7
moving 77:6	notebook 29:7	office 1:1	31:20 33:25	packets 62:23
multilayer 63:6	notes 9:24,25	51:12 76:4	35:3	63:2,19
multiple 31:16	85:11	offices 84:10	organization	page 3:3,7
32:20,23	noticed 10:16	Official 82:3	76:18	10:5,8 16:6,7
33:10 43:14	nowadays	oftentimes	organizations	43:8,17
50:5 55:4	62:18	6:24 44:19	71:4,10	50:11 62:18
75:6 76:9	number 34:24	49:16 50:2	organized	82:20,22,24
79:21	37:25 39:8	53:3,7 60:20	64:22 66:24	83:1,3,5,7,9
	59:22 62:14	61:25	original 42:14	83:11,13
N	69:12 71:16	okay 5:16	59:9	pages 50:10
name 17:8	72:8 75:18	15:21 16:15	originally	82:10
85:14	numbered	16:21 18:12	41:20	paper 70:17,25
named 85:6	34:23	19:13 28:5	output 40:23	71:7 72:13
near 5:5	O	30:23 68:16	40:25 41:3,6	72:18
necessarily	O 84:1	76:2,6,13	outputs 51:24	papers 72:8
52:21	O'BRIEN 2:6	78:25 79:4	outside 49:9	73:11
necessary	O.C.G.A 84:12	old 66:1	51:15	paragraph 6:8
82:10	oath 4:13,15	once 40:1	outsider 52:19	10:20,24
need 5:15	objection	one-way 42:23	53:23 54:6	23:17,17,18
19:20,22		ones 38:6	overflow 51:19	23:19,21,24

24:17 31:11 70:15 paragraphs 23:13 parallel 11:17 11:23,25 part 12:14 13:18 16:7 19:23 21:1 32:18 35:19 72:19,25 parties 39:15 74:1 75:7 84:17 85:12 85:13 parts 19:25 20:25 23:2 party 39:19 42:20 84:14 84:18 pass 81:4 passage 36:20 37:10 password 17:9 25:2,19 26:3 27:2,10 39:8 59:24 60:2 passwords 24:1,4,10,16 24:18,21,22 24:24 25:5,6 25:10,23 26:2,3,9,10 27:3,10 patent 1:1,3,10 1:12,14 2:16 6:7,8,18 7:8 8:10,12 23:16 26:19 26:21,25 27:6,14,20 28:13,14,22 29:3,19 32:11 33:20	68:1,11,21 69:15 patents 7:14 23:13 56:23 Patrick 67:18 69:10 pattern 11:19 12:2,9 57:7,8 57:10,11,13 PC 2:18 PDF 15:17,18 19:7 80:12 Pearson 15:14 people 13:12 14:22 17:5,7 21:8,11 22:11 25:10 26:2,5 39:4 43:7 44:16 56:3 70:12 71:18 perform 58:20 61:25 person 7:4,17 8:17 27:21 27:24 31:20 33:24 35:3 45:22 53:8 67:20,21 personal 30:21 31:7 69:19 personally 56:16 68:2 68:18,24,25 69:9,16 perspective 46:22 petition 69:7 Petitioner 1:7 1:18 2:3 4:8 petitions 6:20 Ph.D 1:17 3:2 4:2 82:15	84:3 phishing 17:12,14,16 17:21 19:14 21:10 70:3 70:14,16 71:2 73:2 phone 30:9 35:23 physical 14:5 44:10,11,12 44:12,15,17 45:2,7,12,17 45:22 46:8 46:15,18,24 47:11 physically 44:20 pick 47:9 picks 23:18 picture 45:22 46:2 piece 51:23 place 49:1 53:17 61:8 85:8 places 29:6 placing 7:16 plan 4:20 5:14 79:8,10 planning 79:8 please 15:21 19:4,12 20:6 20:14,16,23 24:8,14 28:13,16,18 33:7 68:10 69:20 82:9 82:11 point 32:11 poor 27:2,10 73:24 port 65:17 66:4	portion 19:22 63:3 64:17 ports 65:22,25 possibility 53:18 possible 31:3 35:5 38:23 65:10 75:2 potential 9:15 34:1 70:7 potentially 44:23 55:5 63:24 65:19 78:1 practice 14:10 preferred 35:8 preliminary 6:18 prepare 6:17 7:2,12,21 8:1 8:17 9:6 16:16 prepared 9:13 preparing 6:1 6:11 presumably 55:18 70:21 presume 14:23 presuming 37:19 pretend 76:3 pretending 70:23 pretty 56:17 66:7 prevent 30:20 31:6 45:7 49:1 50:18 55:17 61:9 70:18 preventing 26:11 43:24 prevention	11:13,24 12:8 22:15 43:21 prevents 25:15 previous 20:17,23 principles 22:8 37:23 prior 7:18 8:9 9:16 22:23 68:9 85:6 private 39:16 40:2 41:24 58:25 59:3,8 59:12 privileged 30:20,24 31:6 probably 26:16 61:13 62:15 probes 44:23 problem 64:1 problems 5:3 Procedure 82:3 procedures 24:3 53:17 proceedings 6:25 process 48:12 48:12,19,22 48:22,23,24 50:3,9,12,14 51:8 70:19 76:9 process's 49:2 49:2 processed 52:2 processes 47:18 48:15 48:17 50:5,7
---	---	--	---	--

processing 11:18 12:2,9	48:17 49:20 51:3,7 52:15	72:11 84:10 84:14	57:22 64:9	recall 6:12,19
processor 32:4,5 34:6,6 34:10,10,17 34:17,22,22 34:23,24 35:14,17,24 36:1,3,7,13 36:16,20,23 36:25 37:6,7 37:8,13 63:18	55:11 56:6 56:18 57:4 57:24 59:19 60:21 61:6 63:17,23 66:16 67:8,9 71:17 73:2 74:15,20,24 74:24 76:11 77:7,24 78:3 78:9	provided 28:22 29:22 provides 29:9 60:14 providing 27:22,24 60:25 proxy 63:18,25 public 39:13 39:17,21 41:24 58:21 58:22 59:1,4 59:10 83:19	questioning 49:8 questions 4:16 5:11,20 5:23 20:3 51:14 67:16 81:4 quite 14:15	6:22 7:10,22 7:25 8:11,14 9:14 13:5 14:20 21:4 22:1,19 25:25 28:2 46:10 54:20 68:4 69:13 73:19 75:24 80:3,24
processor/s... 35:15 36:17	protected 60:22	58:22 59:1,4 59:10 83:19	R	recalling 6:16 43:4
processors 35:7 76:10	protecting 58:14 61:11 62:2,4 66:19 77:3,11,12 78:1,6	publication 69:24 72:20	RAM 75:22	recess 28:11 54:17 67:14 79:20
produce 74:5	62:2,4 66:19 77:3,11,12 78:1,6	publications 69:25	rates 84:17	recited 34:10
produces 40:23	protection 44:13 50:25 61:2 75:12 75:25 76:5,7 76:13,14,16 76:19,21,22 76:23 77:2 77:18,18 78:9,19,20	published 15:14	re-encrypt 63:20	recites 34:6
professional 71:24	protections 49:1 75:16 75:25 76:9	publishes 39:18	read 10:23 15:23 20:15 20:17 23:20 23:22 31:10 32:13 33:3,6 33:7 36:14 40:2 73:14 82:15,20,22 82:24 83:1,3 83:5,7,9,11 83:13	recognize 21:23 71:10
professionals 71:25 72:1,3 72:4	protects 25:14	pull 11:9	reader 36:2 45:25	recognized 27:21,23
professor 11:4 76:3,12	protocol 40:14 62:19,21 63:8,23 72:25 73:3	purchase 15:16	reading 15:4 15:10	recognizes 25:6
programmer 53:19	protects 25:14	Purdue 11:4	real 69:21 71:1 71:4	recollection 8:5 9:4 12:19 12:22 15:10 17:13 22:2 71:7
programmers 53:15	protector 40:14 62:19,21 63:8,23 72:25 73:3	purpose 73:25 75:19	realizing 17:10	record 16:20 17:15 20:18 46:6,17 54:16 57:21 67:12,13 73:20 80:20 80:21
programming 53:15	protocols 62:3 65:5 67:6	purposes 79:8	really 25:18 66:18 67:7 67:16 70:19	reduce 53:18
programs 53:20	prototype 71:5 71:8 72:21	Pursuant 82:2 84:5	reason 4:21,25 16:10 82:21 82:23,25 83:2,4,6,8,10 83:12,14	reduced 85:9
prohibited 84:12	provide 4:22 38:18 42:17 49:19 61:1	put 44:23 45:15 53:17	reasons 82:7	redundancy 43:12
project 11:17 12:1 71:4		Q		refer 50:10,15
pronounce 42:11		quality 27:2,10		reference 22:24 69:15 69:17
property 41:11 43:6		question 5:11 5:12 14:15 19:19 20:7,9 20:20 23:7 25:22 27:17 28:2,4 32:16 33:4 45:6		
protect 22:25				

references 8:9 9:16 68:9 69:8,9,12,13 referral 84:15 referred 13:9 13:12 30:1 40:24 referring 17:20 20:20,24 21:2,3 51:21 57:6 58:2 refers 50:8 65:21 reflect 14:18 refresh 15:10 refreshed 31:18 33:13 refreshes 30:17 regular 85:12 Regulations 84:6 reject 32:17 rejection 32:8 relate 38:8 related 33:4 67:16 73:21 release 58:5 released 41:20 releasing 58:6 relied 19:22 remember 7:20 12:17 12:20 20:4 25:7 69:11 REMOTE 1:17 remotely 7:3,5 8:16,19 render 27:3 Renee 1:24 15:25 84:22 85:4,19 reopen 19:18 rephrase 23:6	46:24 50:19 report 23:11 Reported 1:24 reporter 15:25 16:14 20:14 20:16 84:8 84:14 85:4 reporting 84:6 84:11,14,14 representative 84:8 represented 29:24 representing 7:8 reputation 68:20 69:1 requested 18:2 requests 43:23 requires 4:15 research 70:25 72:6 researchers 22:10 resource 36:8 respect 76:20 respective 29:12 respond 71:10 responding 32:18 response 20:17,20,23 36:23 responses 6:18 8:10,13 restrict 49:17 53:7 restricted 35:16 36:18 36:24 37:2,9 restrictions	30:19 37:7 48:3,8,9 result 21:14 85:13 retailer 29:17 reuse 27:2,10 reveal 21:13 revealing 17:8 21:8 25:16 reverse 41:5 reversed 59:2 review 6:2,10 6:18,20 8:4 8:10,12 9:2,7 9:9,12 32:12 80:1 reviewed 6:13 6:22 8:2,5,6 8:8,8 9:5 67:17 reviewing 6:12 10:11,16 right 4:19 12:12,25 13:1 16:9,18 16:23 19:24 20:25 24:4 26:16 29:13 31:25 32:16 32:21 34:7 37:2 45:14 52:23 53:23 54:2,19 64:5 67:18 68:12 70:25 79:12 79:17 80:9 rights 39:5,6 48:23 53:4 61:7 75:15 ring 69:6 risk 66:4 RMR 1:24 84:22 85:19 Roberto 14:2	15:14 robust 48:7 55:13 roles 53:4,6,9 room 44:16 rooms 44:14 rough 7:23 roughly 7:20 13:25 RPR 1:24 84:22 85:19 Rule 82:2 rules 4:11 82:3 84:5 run 40:22 42:15 running 18:23 48:14,18 66:15	57:25 59:20 61:3,22 62:13 63:10 64:19 66:9 66:22 73:17 74:22 76:15 76:24 78:11 78:21 scratch 21:21 52:16 64:15 screen 9:23 se 45:16 second 18:20 32:5 34:6,10 34:17,22,23 secret 39:7,10 39:15 42:13 42:16,21,22 74:1,5 section 27:6 32:11 45:4 49:11 51:17 52:18,19,22 53:24 54:1,3 65:16 66:8 sections 10:1 64:11,17,22 secure 24:22 27:3 35:14 35:21,25 36:9,16,20 36:22 37:5,8 37:12 47:21 securely 25:11 secures 34:21 security 3:9 11:2,11,23 12:4,6,7,21 12:25 13:4,8 13:10,13,15 13:17,18 14:1,5,5,6,7 14:9,10,11 14:13,14,19
---	--	---	---	---

15:1,13 17:2	42:2,19 59:8	sessions	79:21 81:3	site 29:16
17:5 21:17	60:22 63:7	63:15	shoes 7:16	sites 30:1,3
21:19 22:10	63:21 70:6	set 5:20,23	short 26:2	sitting 8:14
25:21,23	80:9	55:5 64:24	shorter 24:22	22:19 49:6
26:2 27:22	sender 22:6,6	85:8	shorthand	size 52:6
27:25 37:16	sending 18:6	setting 65:19	85:9,11	skill 7:17
37:16,23,25	63:14 70:20	share 15:19	show 33:19	27:21,24
38:4,8,10,10	sends 39:22	42:13 74:1,5	showing 33:23	31:20 33:25
38:12,18	sensitive 21:9	shared 30:21	shown 29:23	35:3
44:9,10,11	49:16 61:6	31:7 39:15	35:23	slippery 63:11
44:12,17,18	61:11 74:15	41:15	shows 24:24	slope 63:12
45:2,7,12,17	74:21	shares 58:23	34:1,16,22	smaller 35:25
46:8,15,18	sensor 25:9	sharing 37:18	45:25	Smith 2:18 7:6
46:25 47:16	35:18 36:1	50:5	sic 26:19	7:6,7
47:25 48:2	sent 16:21	sheet 82:12	28:13 44:9	social 14:25
48:12,13	18:18 19:21	Shi 2:5 3:4 4:6	sign 10:11	17:1,3 19:15
49:3,12,14	31:25 32:3	4:7 16:4,14	42:1 56:8,9	21:5,7,7,15
49:23 50:18	42:22,24	16:25 17:19	57:3 58:5	21:23 22:12
50:21 51:7	56:2 58:10	17:22 18:18	signature 10:8	22:16,22,25
53:1,2,11	59:14 62:23	18:22 19:20	42:3,5 55:20	23:4,10 24:5
54:5 61:17	sentence	20:16,19,22	55:21 56:12	24:13,19,25
61:20,21	10:23 23:23	22:14,21	56:25 57:2,3	25:2,15,21
62:8,11 63:5	31:11 32:13	23:6,8 24:8	57:7,15,15	26:6,11,14
66:7,7,14,18	33:3,6,7,14	28:5,10,12	57:16,23	26:20 27:1
66:19 67:23	33:15	29:13 31:10	58:3,8 59:6	27:11,15,18
69:25 70:11	separate 5:22	33:3 34:5,19	59:15 73:22	27:25 29:15
71:14 72:2	server 43:13	36:12 37:15	73:24 74:4	44:2 45:3,5,7
72:11 73:14	43:13,14,16	38:20 40:18	83:17	45:13,18,24
74:11	servers 66:17	44:7 46:7,18	signatures	46:9,20 47:3
see 16:9 17:17	67:10	47:3,15	41:23 58:20	49:4 69:19
32:7 34:15	service 29:17	50:17 51:17	59:17	69:21 70:5
37:20 39:5	30:6,7,10,13	54:10,13,16	signed 15:20	71:11,19
46:1 49:12	30:25 31:15	54:18 55:20	42:5	software 11:2
49:21 51:2	31:24 32:2	57:18,22	similar 4:11	17:10 21:20
59:11,13	32:14,20	58:16 60:9	60:17 72:2	41:18,19
60:2,7 61:17	37:14 43:21	61:10 62:6	simple 51:18	42:2,2 47:18
64:12 65:23	43:25 55:8	63:4 64:2	simply 40:15	47:22 48:3
68:22 79:17	65:7	65:12 66:6	single 29:25	48:15 53:15
seeing 32:9	services 29:10	66:18 67:11	31:16 33:11	53:17,19
segments	29:25 84:8	67:15 73:21	69:14	54:22 56:1,2
50:10	84:10,11,11	75:5 76:22	sit 6:16,19	56:7,8,9,10
selection 27:2	84:13,14,16	77:11 78:18	7:11 20:8	56:12,17,24
27:10	session 62:21	78:25 79:4,7	41:9 43:4	57:4,9,13,19
send 39:20	73:5	79:12,14,19	61:15 69:6	58:4,5,6,9,10

58:12,15	27:18 67:1	12:2	sworn 4:1,3	tactics 19:15
59:7,9,10,13	78:23	student 11:3	85:7	take 16:15,19
59:14 60:17	specification	71:6 76:3	synchronize	28:6 40:22
60:21 66:1	26:22	students 13:2	31:17 33:11	42:14,21
66:15	speculating	13:22 22:2	synchronized	43:12,16
solution 22:25	7:24	22:15	30:12,16	54:12,13
solutions	spend 28:3	studied 7:14	system 14:5	59:7 67:12
22:16,22	spent 7:21	sub-concepts	18:3 21:19	78:25 79:2
somebody	sphere 72:1	38:1	24:23 25:8	taken 1:18
21:17 40:11	spoken 79:22	subcompon...	26:11 28:21	28:11 54:17
40:16 43:21	spread 54:23	38:17	34:2 38:13	67:14 79:20
45:8 55:14	54:24	submit 16:10	38:20 43:7	79:21 85:8,8
70:19,23	stack 14:7,8	subscribed	43:22 47:15	85:11
72:17	64:23 66:25	85:14	47:17,19,20	talk 7:9 17:3,5
soon 16:24	67:3	substance	47:22,24	25:24 36:20
sophomores	stands 38:2	82:5	48:2,4,5,7,9	47:6,7 65:3
13:6	start 12:21	substantive	48:14,16,18	65:10,17
sorry 14:16	20:22	10:18,18	49:3,12,14	69:18 70:14
17:16,22	started 12:22	subterfuge	49:19 51:23	76:4,10
18:9 20:21	starting 31:11	17:6	52:3 53:5	talked 41:25
46:3 64:15	35:11 64:25	suggested	54:9 61:8	58:1,21
75:24 76:11	State 84:2 85:2	32:17	70:1 72:20	61:12 71:12
Sounds 79:6	85:4	suite 2:10,19	73:6 76:7,14	72:22 73:18
source 36:10	statement	12:14	76:17,18	75:13,14,15
57:5	82:7	supervision	77:19	75:17,25
Southern 5:4	states 1:1 24:1	85:10	systems 21:21	76:5,7,8
space 48:20	30:9 36:15	supplemental	24:3 38:18	77:16,22
50:4,9 51:8	steps 33:18	82:10	45:7 63:16	78:2
52:13	stick 6:25	supporting	71:18	talking 7:10
speak 6:5	storage 29:17	69:8,9,12,13		28:12 30:15
23:11 68:20	30:6,7,10,13	69:14	T	54:19 56:22
69:2	30:25 31:14	supports	T 1:17 3:2 4:2	57:16 66:13
speaking	31:24 32:2	37:11	15:13 82:1,1	68:5
24:21 61:4	32:14,19	sure 5:25 11:8	82:14 84:3	talks 70:16
61:23 64:6	33:9 34:21	25:4 28:19	85:1,1	Tamassia 14:2
74:12 77:10	35:14,22,24	33:8 41:16	T-A-M-A-S-S...	15:14
speaks 32:4	35:25 36:16	41:18 55:15	14:2	tampered
specific 4:12	37:14	65:16 68:11	T-R-I-C-E-R-T	56:14
5:22 9:18	stored 30:20	69:23 72:13	70:2	taught 10:25
13:14 23:2,8	30:24 31:7	surprising	table 3:8 15:22	11:6,10 12:3
27:25 57:20	31:22 39:3	13:19	16:5 19:21	12:5,13,17
68:10 76:17	Street 2:19	swapped	20:2 37:17	13:4 14:20
78:12,15	structures	50:13 51:5	37:22 44:8	14:22 15:11
specifically	11:1,14,18	51:10	48:11 61:19	15:11 21:6

24:23 37:5 66:8 71:14 71:23 72:2 teach 12:21 22:15 38:9,9 71:17 teaches 25:12 27:1 teaching 12:11 12:15,22 14:22,23 27:9 Tech 71:21 technical 6:25 22:16,21,25 technically 62:16 66:11 technique 24:5,19 25:20 27:8 50:7 56:17 58:13 62:7 70:17 73:10 73:14 77:17 77:23 78:3,5 techniques 21:17 22:12 26:13,18,24 27:14 50:18 51:7 64:2,4,9 72:10,14 75:11,19 76:1,10 77:11,12,13 77:17 78:8 78:14,18 technologies 23:3,8 72:7 technology 50:15 67:16 71:3 73:7,8,9 tell 20:23 22:2 73:16 ten-minute	28:6 54:13 tend 57:8 tends 57:13 test 20:5 testified 4:4 testify 85:7 testimony 4:22 79:25 82:6 Texas 2:11,20 text 11:18 12:2 12:9 37:21 39:24 52:1 textbook 12:6 13:17,20 14:1 15:3,10 15:12 19:10 19:13,18,25 20:7 21:1 71:13,14,16 71:22 thank 5:9,16 15:25 16:8 17:19 18:13 18:17 28:10 51:13 54:4 54:15,16 67:11 79:16 79:19 81:6 thing 32:8 70:12 73:13 things 9:23 17:5,11 22:5 38:9 44:25 47:12,14,18 53:8 55:1 56:22 57:11 60:17 64:6,7 66:17 78:24 think 5:5 13:12 45:16 46:11 46:14 60:24 67:12 73:13 74:17 78:23 thinking 7:16	21:12 61:14 third-party 29:17 45:23 45:25 60:16 60:23 thought 46:11 46:13 73:23 threads 48:14 three 38:1,6,16 38:20 thwart 45:18 46:9,14 53:11 tied 66:7 time 5:15 9:5 10:19 14:20 28:3 78:22 79:18 80:19 85:8 title 15:12 titled 61:16 today 4:13,19 4:23 5:1,17 6:16,19 7:11 8:1,15 9:9 20:8 22:20 41:9,22 43:4 49:6 56:9,23 56:25 57:17 58:13 59:16 59:22,23 60:11,20 61:4,14,15 61:24 62:10 63:12 64:1,9 66:4 69:6 73:19,20 74:13 75:14 75:19 76:11 76:20 78:1,6 79:9,11,22 80:5,16,18 80:23 81:1 today's 9:6	told 20:5 tool 39:13 40:4 40:9,10,20 42:10 43:20 48:5 60:14 61:5 80:13 tools 39:11 40:18 41:7 41:21,22 42:7 43:1,10 43:11,18,24 43:25 47:24 48:1,6 50:21 55:9,11 59:22 60:10 60:23 61:10 top 65:1 67:3 topics 12:5 13:14,21,24 14:3,24 15:3 15:4,11,23 17:4 20:2 21:4,5 72:3 totality 6:21 TRADEMARK 1:1 transcript 17:18 85:10 transcription 85:9 transfer 73:7,9 transit 39:23 translation 28:21 29:9 29:22 translator 28:23,25 29:8,12,18 translators 29:5 transmission 63:4,5 64:3 transmitted 39:3	trends 14:18 TRIAL 1:3 TRICERT 70:2 72:14 trick 17:7 21:8 21:11 22:11 26:5 70:9 tricked 21:14 45:8 tricking 21:17 tried 6:25 13:21 60:6 true 39:25 41:13 53:14 77:10 82:17 85:10 truly 74:2 trust 70:22 trusted 72:17 truth 85:7,7,7 truthful 4:22 truthfully 4:16 4:18 try 15:24 20:4 23:14 55:4 70:9 trying 22:13 43:22,23 48:8,10 51:1 53:11 65:6,7 70:23 79:10 turn 44:21 turns 66:10 two 7:21 8:5 16:19 39:15 42:12 43:2 51:25 64:22 73:25 type 39:7 55:24 57:2 57:20 58:21 types 19:15 53:8 59:1 62:1 64:12
---	---	---	--	---

71:11	unrelated 68:7	variety 24:10	20:10,13	widely 39:18
typical 7:15	updates 31:17	29:6,23,25	32:16 39:3	61:14
typically 24:2	33:12	45:13 65:10	40:24 45:16	wifi 63:1
26:8 48:20	upload 15:21	various 31:11	45:16 58:8	wild 5:4,7
62:18	upper 13:7	31:14 33:9	61:1 64:21	willing 32:11
typos 10:17	usability 14:4	62:1,10 64:9	64:21 66:24	window 16:11
	use 17:5,6	65:22	68:14 76:19	wish 10:18
U	18:3,4 21:7	verification	76:25 85:13	wishes 39:20
U 84:1	24:24 25:5,6	42:6	ways 22:11	witness 3:2
U.S 1:12,14	26:2 30:13	verify 22:3,6	58:19 62:14	4:1 16:15,18
6:6	37:9 40:1	42:4 73:2	63:13 70:5	16:21 19:18
UCI 71:23	41:22 50:7	74:6 75:7	70:13 73:1	20:13 22:1
ultimate 53:16	58:17,17,24	version 60:7	78:15	22:19 24:7
ultimately	59:3,4,18,22	versus 78:16	we'll 39:16,19	28:9 29:2
72:21	62:2,19,20	victim 70:7	42:1	31:2 32:23
unchanged	63:8 64:7,8	Videoconfer...	we're 5:3,17	33:17 34:13
41:12	67:6 73:3	1:22,25 2:5,6	28:5 49:25	36:6 37:4
undergradu...	75:19 76:11	2:7,17	56:22 57:6	38:16 40:7
10:25	77:25 78:6	view 19:1	66:13 70:10	44:5 47:6
undergradu...	78:14 80:12	Virginia 71:21	70:10	49:25 50:24
13:5,24	82:9	virtual 49:23	we've 54:10	54:8 55:11
undersigned...	useful 53:3	50:7,15,17	67:23	56:21 58:1
82:14	user 17:8 24:2	50:20 51:6	weak 26:9	59:21 61:4
understand	25:10 30:18	76:5	web 14:8 43:8	61:23 62:14
4:13,15	36:8,12,22	virus 41:17	43:12,13,14	63:11 64:20
13:23 31:21	37:6 52:2	55:25 56:5	43:16,17	65:16 66:10
35:4	53:5 54:25	56:15,24	62:18 66:7	66:23 73:18
understandi...	65:13	58:12 63:19	66:18	74:23 76:16
5:19	users 25:5	70:8	website 25:11	76:25 78:12
understood	35:13 36:15	viruses 57:8	25:13,14,17	78:22 79:2,6
33:24	53:4	57:14 58:14	29:16 43:8	79:17 81:4
unencrypted	uses 25:1	63:14,25	43:12 52:1	85:6,14
59:9 60:7	45:10 58:25		55:8 62:22	wonderful
64:4,8	usual 84:17	W	66:12,16	51:13
unfortunately	usually 26:7	W 2:6	73:4	word 57:7
63:12	55:2	want 5:7 16:12	websites	work 11:3 15:8
UNITED 1:1	utilize 72:9	28:3 34:15	21:12 22:3	55:23 62:12
universities		41:16 43:7	34:14 66:14	68:19 69:1
71:17	V	48:25 51:3	67:6,8,9	69:22 72:6
University	v 1:8	52:15 53:7	week 8:22	79:4
11:5 71:20	valid 55:16	53:17 55:15	went 13:20	working 60:18
71:20,21	56:12 73:4	60:20 77:7	WHEREOF	works 73:25
unlock 25:9	value 39:25	wants 58:23	85:14	79:1
39:8 47:10	41:5 42:24	way 18:21 20:1	wide 24:10	world 69:21

71:1,4 worm 54:21,22 55:2,17 worms 55:9,12 wouldn't 45:15 wrap 79:14 wrapped 37:25 writing 53:20 written 71:13 wrote 13:19 59:7 64:21	33:24 34:5,9 34:11,13 35:2 37:12 44:7 61:17 61:19 80:9 80:16 1.4 54:1 10,925 6:7 10,929,512 1:12 10.B 84:5 1006 68:11 1007 68:21 1008 69:3 1009 69:15 102 29:7,14,23 30:6,9 31:23 32:1 35:1 104 29:10 30:9 108 29:10,24 11,514,138 1:14 110 29:25 12:02 1:20 120 29:16,25 30:1,5 122 29:16 124 29:17 30:1 30:1,5 132 29:8 136 29:18 138 5:18 23:13 140 29:17 30:6 30:7,11,14 30:25 31:15 31:24 32:2 32:14,20 33:9 37:14 15 6:8 1500 2:10 16 3:9 1983 11:4 12:12,15 1990s 12:19	12:23 2 2 29:4,19 44:10 2000s 12:23 2011 15:14 2025 1:19 83:20 85:14 2037 10:3 2100 2:19 3 3 29:3 34:18 34:19,20 35:1,7,9,10 35:21,22 52:19,22 3.2 48:11 3.3 49:11 3.4 51:17 3.4.2 51:18 3:20 79:5,18 30(e) 82:2 300 35:23 302 35:24 303 2:19 304 34:23 35:7 35:25 36:3 37:7 306 35:25 308 34:24 35:7 35:18 36:1 36:13,25 310 36:1 33 23:17,21,25 24:17 34 23:17 35 27:7 37 29:20 4 4 3:4 35:12 36:15 37:10 52:22 54:19	4.1 52:18 54:3 4:24 81:7 44 27:7 45 23:18 5 5 33:22 35:13 36:14 61:16 64:11,17 67:1 5:00 79:11,12 79:15 51 26:19 28:13 28:14 512 2:12,21 5:18 6:7 10:3 19:8 23:12 23:16,22 26:21,24 27:6,9,14,20 27:23 28:14 28:22 29:3 29:19 68:1 56 31:13 33:6 33:9 6 6 33:21 62:17 64:11,17 67:1 6.4.4 65:16 60 23:19 30:9 62 30:17 66 35:11,20 692-8700 2:21 7 7 30:8 31:14 33:6,21 66:8 66:14 67:7 78701 2:11,20 8 8 1:19 10:20 10:24	867-8440 2:12 8th 85:14 9 9-11-28 84:12 9-11-30(e) 82:4 929,512 6:7 98 2:9
---	---	--	--	---