

1 UNITED STATES PATENT AND TRADEMARK OFFICE
2 BEFORE THE PATENT TRIAL AND APPEAL BOARD
3 SOPHOS LTD. and SOPHOS INC.,

4 Petitioners,

6 v.

8 OPEN TEXT INC.,

9 Patent Owner.

10 -----
Case No. IPR2023-00699

11 Patent No. 8,418,250

12
13 Deposition of

14 DR. RICHARD NEWMAN

15 Conducted Virtually

16 Thursday, December 7, 2023

17 9:32 a.m. EST

18
19
20 Job No.: 516887

21 Pages: 1 - 162

22 Reported by: Cassidy Western, RPR

1 Deposition of DR. RICHARD NEWMAN, conducted
2 virtually.

3
4
5
6
7
8 Pursuant to notice, before Cassidy Western,
9 RPR, Notary Public in and for the Commonwealth of
10 Pennsylvania.

A P P E A R A N C E S

ON BEHALF OF THE PETITIONERS, SOPHOS LTD. AND
SOPHOS INC.:

VIVIAN LU, ESQUIRE

GIBSON DUNN & CRUTCHER LLP

200 Park Avenue

New York, NY 10166

(212) 351-4000

and

BRIAN M. BUROKER, ESQUIRE

GIBSON DUNN & CRUTCHER LLP

1050 Connecticut Avenue, N.W.

Washington, D.C. 20036

(202) 955-8500

ON BEHALF OF THE PATENT OWNER, OPEN TEXT
INC.:

RUSSELL E. BLYTHE, ESQUIRE

KING & SPALDING LLP

1180 Peachtree Street, NE, Suite 1600

Atlanta, GA 30309

(404) 572-4600

1 A P P E A R A N C E S (continued)

2 ALSO PRESENT:

3 Manita Joseph, A/V Technician

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

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

C O N T E N T S

EXAMINATION OF DR. RICHARD NEWMAN	PAGE
By Mr. Blythe	6

E X H I B I T S

NEWMAN DEPOSITION EXHIBIT	PAGE
Exhibit 1 Patent Owner Open Text Inc.'s Notice of Deposition of Dr. Richard Newman	9
Exhibit 2 CV of Dr. Richard Ernest Newman	11
Exhibit 3 Declaration of Dr. Richard Newman in Support of Petitioners in the Petition for Inter Partes Review of U.S. Patent No. 8,418,250	35
Exhibit 4 U.S. Patent No. 8,418,250	39
Exhibit 5 U.S. Patent Application Publication US 2004/0111632 A1	69

1 DR. RICHARD NEWMAN,
2 of lawful age, being first duly sworn or affirmed
3 to testify to the truth, the whole truth, and
4 nothing but the truth, was examined and testified
5 as follows:

6 EXAMINATION BY COUNSEL FOR THE PATENT OWNER
7 BY MR. BLYTHE:

8 Q Good morning.

9 A Good morning.

10 Q Please state your name for the record.

11 A Richard Ernest Newman.

12 Q And what is it? Dr. Newman?

13 A Richard Ernest Newman.

14 Q And is it Dr. Newman? Is that the
15 correct title?

16 A Oh, yes.

17 Q Okay. What is your address, Dr. Newman?

18 A 8524 Southwest 23rd Place in
19 Gainesville, Florida 32607.

20 Q Where are you sitting today?

21 A I'm in the offices of Gibson & Dunn in
22 New York City.

1 signal can be analyzed to attempt to detect
2 malware.

3 BY MR. BLYTHE:

4 Q In paragraph 40, you say:

5 "When an unknown program, or a modified
6 version of a known program executes, either it or
7 the system as a whole may be monitored for
8 behavior to determine whether or not the attempted
9 or actual behavior is normal."

10 Do you see that?

11 A Yes.

12 MS. LU: Objection; form.

13 THE WITNESS: Yes, I see --

14 BY MR. BLYTHE:

15 Q And you agree with --

16 A Yes.

17 Q -- that? And you agree with that
18 statement still. Correct?

19 A Yes.

20 Q Okay. So in other words, one approach
21 to malware detection is to look at the behavior of
22 a system as a whole and determine whether it may

1 be infected with malware. Is that right?

2 A That's correct.

3 MS. LU: Objection; form.

4 THE WITNESS: That's one way you can do
5 it.

6 BY MR. BLYTHE:

7 Q All right. And another approach is to
8 look at a specific object and determine whether
9 the behavior of that object indicates that it's
10 malware. Is that correct?

11 A Yes, that's correct. There are other
12 forms as well where you might look at a collection
13 of objects to see if that particular collection
14 exhibits anomalous behavior or bad behavior.

15 Q Okay. Let's now flip over to
16 paragraph 46 of your declaration.

17 A Okay. I'm there.

18 Q Okay. In paragraph 46, you include an
19 overview of what is disclosed in the '250 patent.
20 Is that correct?

21 MS. LU: Objection; form.

22 THE WITNESS: Yes, I would say that,

1 things. So examples that are given include
2 viruses and worms and Trojan horses. But there
3 are others besides that.

4 Q What is a "computer object" in the
5 context of the '250 patent?

6 A Well, I found that somewhat interesting.
7 Referring to the '250 patent, Column 7, Line 63,
8 there's a sentence that begins:

9 "An object in this sense may be a
10 computer file, part of a file, or a subprogram,
11 macro, web page or any other piece of code to be
12 operated on -- operated by or on the computer or
13 any other event, whether executed, emulated,
14 simulated or interpreted."

15 I would add to that -- if it were me, I
16 would -- I don't know that I would say "event" in
17 there, personally. But that's what the '250 says.
18 And I would also include network packets, frames,
19 or parts thereof as objects, for example.

20 So I -- you know, I think, on the one
21 hand, that it's not -- it's not an exhaustive
22 list, on the one hand, but it also includes

1 MS. LU: Objection; form.

2 THE WITNESS: So I don't see any wording
3 offhand that talks about monitoring that -- as a
4 system as a whole or where it says that that's an
5 object. But the '250 patent refers to objects as
6 what they're monitoring and talks about, in
7 Column 14, about speed of propagation and
8 propagation of -- propagation of malware. But
9 they also talk about propagation of events. And
10 the volume of infection can be used as a trigger.

11 Now, as I'm sure the author of '250
12 knows and your expert knows, a very common thing
13 for stealthy viruses and worms to do is to rename
14 themselves or to change their appearance so that
15 it's more difficult to detect them.

16 And so in order to measure the
17 propagation of malware, you'd have to be able to
18 associate derivative objects. So a particular
19 piece of malware might be executed and what
20 viruses and worms do is they copy themselves. A
21 virus will attach itself to another object. A
22 worm does not need to do that and can send itself

1 that.

2 So in your interpretation of the claims
3 of the '250 patent, when it refers to data that
4 includes information about the behavior of the
5 object running on one or more remote computers, is
6 it your view that that refers to the operation of
7 the system as a whole?

8 MS. LU: Objection; form.

9 THE WITNESS: I would say that it's
10 directed at a particular file, the processes
11 executing that file, or attachment, if you will,
12 and -- or part of an attachment like a macro. You
13 can have macro viruses in, say, Word or Excel or
14 something of that nature. And since they include
15 events, I'd say object -- you'd have to monitor
16 not just the executing code for that, but all its
17 derivatives and events that it spawns, each of
18 which could be considered an object under the '250
19 patent.

20 But not -- the '250 patent, as I recall,
21 does not talk about overall system characteristics
22 like number of processes on the system or the

1 paging rate or something of that nature.

2 MR. BLYTHE: Okay. Let's take a break.

3 (Whereupon, there was a recess in the
4 proceedings.)

5 BY MR. BLYTHE:

6 Q Dr. Newman, we just finished with a
7 break. Did you have any discussion with Counsel
8 regarding the substance of your testimony while we
9 were on break?

10 A I told her what I thought about things
11 so far, and she said nothing to me. Basically,
12 she said I can't talk to you about this.

13 Q Okay. Let's pick back up with paragraph
14 46 of your declaration.

15 A Okay.

16 Q In paragraph 46, you refer to
17 classifying a computer object as malware. Do you
18 see that?

19 MS. LU: Objection; form.

20 THE WITNESS: Yes, I see that.

21 BY MR. BLYTHE:

22 Q What does it mean to classify a computer

1 Q All right. Turn to paragraph 81 of your
2 declaration.

3 In paragraph 81 of your declaration, you
4 state that:

5 "The method in Halperin compares the
6 suspect object to predefined criteria that are
7 characteristics of malicious software."

8 Do you see that?

9 A Yes.

10 Q Okay. Halperin compares behavior
11 information to predefined criteria. Correct?

12 MS. LU: Objection; form.

13 THE WITNESS: It says "correlated target
14 behavior correspond to predefined suspicious
15 behavior patterns," so -- of target behavior,
16 yeah.

17 BY MR. BLYTHE:

18 Q But Halperin does not compare an object
19 to predefined criteria, does it?

20 MS. LU: Objection; form.

21 THE WITNESS: Halperin uses this
22 predefined criteria as behavioral indications of

1 the presence of malware. So if we treat events as
2 objects, then I would say yes. If we treat
3 files -- only files as objects, or if we're
4 looking at that in a narrower sense, then Halperin
5 uses the behavioral indications to indicate the
6 presence of that -- of a malware object, which
7 then the system attempts to identify in other
8 ways.

9 BY MR. BLYTHE:

10 Q Okay. Where in your view, does Halperin
11 disclose comparing an object to predefined
12 criteria?

13 MS. LU: Objection; form.

14 THE WITNESS: Well, aside from what I
15 already mentioned about events, certainly events
16 are being compared to predefined criteria in the
17 behavioral profiles in the audit activity that's
18 going on there.

19 But if you look at -- so in paragraph 61
20 of Halperin, it's on the next page, up at the
21 second column at the top, so it says:

22 "It is believed that such

1 BY MR. BLYTHE:

2 Q So Halperin there discloses identifying
3 that a virus exists in the system. Right?

4 A It says --

5 MS. LU: Objection; form.

6 THE WITNESS: Thank you.

7 It says, "identify a previously unknown
8 virus." And then it says "if one system detects a
9 suspected virus," et cetera, and "the system
10 operator has to indicate that this suspected
11 activity is truly a virus."

12 So a virus is a piece of code that is
13 capable of replicating itself and attaching
14 itself, and, in fact, it must attach itself to
15 some other object. So you can talk about viral
16 behavior. And in the '250 patent, they talk about
17 events as objects, and so in that sense it's an
18 object, I would say it's a more narrow sense. And
19 my preference would be to refer to objects as only
20 things like files or pieces of files or something
21 that can be stored in the tangible meaning, that
22 sort of thing.

1 existing profiles.

2 And then an operator looked at this
3 forensic analysis, told him that there's a virus
4 operating in the system, and then you go back to
5 find out when this thing first arrived and when
6 you got rid of it. And the operator would then
7 indicate that these periods were -- are not to be
8 used for learning what normal looks like.

9 BY MR. BLYTHE:

10 Q Okay. Paragraph 87 of Halperin says, in
11 part:

12 "In addition, the system gets
13 retrospective external inputs from an operator or
14 standard antivirus software on when there was a
15 virus in the system."

16 A Yes.

17 Q Do you see that?

18 A I do.

19 Q Is it your testimony that the
20 retrospective external input would come from the
21 Halperin system itself?

22 MS. LU: Objection; form.

1 THE WITNESS: I'm saying that the
2 operator's input could be informed by Halperin's
3 system.

4 BY MR. BLYTHE:

5 Q Okay.

6 A So the prob- -- the problem is this.
7 You run -- you're looking for anomalies, okay? So
8 when you're looking for malware, the antivirus
9 signature detectors, you know, anti-viral software
10 has to update their signature database because new
11 malware is detected all the time and they have to
12 add new signatures.

13 The -- when you're looking for
14 anomalies -- when you're looking for anomalous
15 behavior, you need to know what normal looks like.
16 You have to have some sense of what is expected
17 behavior. And expected behavior changes over time
18 with different users coming and going, different
19 equipment coming and going, different software
20 coming and going, different network equipment, and
21 so on. So things change. And you need to look at
22 how -- you need to change what normal looks like

1 MS. LU: Objection; form.

2 BY MR. BLYTHE:

3 Q And then it states:

4 "If the calculated value is lower than
5 the predefined threshold, the system can activate
6 a virus alarm and possibly initiate virus
7 containment actions."

8 Right?

9 A Yes, that's what it says.

10 Q All right. So is the result of this
11 determining phase, identifying a specific object
12 as malware?

13 MS. LU: Objection; form.

14 THE WITNESS: It's identifying the --
15 well, it's computing the likelihood that there is
16 malicious behavior that is taking place. And --

17 BY MR. BLYTHE:

18 Q But not classifying a specific object as
19 malware. Correct?

20 A Again --

21 MS. LU: Objection; form.

22 THE WITNESS: -- it's not identifying a

1 particular file as malware at this stage. If you
2 take events as objects as the '250 patent
3 apparently does, then yeah. It's identifying the
4 event object as it being in existence.

5 And no doubt it would say which of the
6 sensors were major contributors to this
7 low-probability event or low-probability
8 occurrence, combination of events.

9 BY MR. BLYTHE:

10 Q Okay. Let's look back at the '250
11 patent and Dependent Claims 2 and 14. I'm going
12 to pull that up. We'll start with Claim 2.

13 A Okay.

14 Q All right. Claim 2 further limits
15 Claim 1 by stating that:

16 "The data about the computer object that
17 is sent from the plural remote computers to the
18 base computer includes one or more of certain
19 items listed there."

20 Do you see that?

21 A Yes, I do.

22 MS. LU: Objection; form.

1 However --

2 BY MR. BLYTHE:

3 Q Halperin (indiscernible) --

4 A -- I think -- go ahead.

5 Q Halperin does not expressly refer to
6 naming any specific computer objects, does it?

7 MS. LU: Objection; form.

8 THE WITNESS: Well, Halperin talks about
9 isolating a source of the infection or the
10 activity, and it is hard to see how you could say
11 the same attachment is sent to multiple computers
12 that exhibit the same behavior and not have the
13 analysis include some way of identifying that
14 those are -- that those attachments are either the
15 same or similar, as Halperin says in -- in the
16 list of suspicious behaviors.

17 BY MR. BLYTHE:

18 Q Well, you could use a hash. Right?

19 A You could use any one of a number of
20 things. Name is one. A very common one.

21 Q But Halperin -- okay. But Halperin
22 doesn't expressly say anything about identifying

1 the name of a specific computer object. Correct?

2 MS. LU: Objection; form.

3 THE WITNESS: I don't cite anything
4 there that says that. But -- but there may be
5 indications of that in Halperin that -- that I did
6 not cite.

7 BY MR. BLYTHE:

8 Q And Halperin doesn't say that
9 identifying the name of an object is a suspicious
10 behavior pattern. Correct?

11 MS. LU: Objection; form.

12 THE WITNESS: Halperin doesn't use the
13 four-letter-word, "name." But 44, paragraph 44
14 says, "sending a file attached to a message
15 several times from the same user."

16 How would you know it's the same file
17 that's attached to these different messages?

18 BY MR. BLYTHE:

19 Q Well, you'd use a hash. Right?

20 MS. LU: Objection; form.

21 THE WITNESS: Using a hash is one way
22 that you could do that and would be effective if