

In The Matter Of:

SYMANTEC CORPORATION

v.

***THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY
OF NEW YORK***

GOODRICH, Ph.D., MICHAEL T. - Vol. 1
August 24, 2015



Court Reporting Solutions

20750 Ventura Boulevard, Suite 205
Woodlands Hills, CA 91364
Phone: 818.593.2300 - Fax: 818.593.2301

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

SYMANTEC CORPORATION;)	
)	
Petitioner,)	
)	
vs.)	Case No.
)	IPR2015-00372
THE TRUSTEES OF COLUMBIA)	
UNIVERSITY IN THE CITY OF)	VOLUME I
NEW YORK;)	
)	(Pages 1 - 300)
Patent Owner.)	
_____)	

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

Newport Beach, California

Monday, August 24, 2015

Reported by:
Lynda L. Fenn, CSR, RPR
CSR No. 12566

Page 2

1 UNITED STATES PATENT AND TRADEMARK OFFICE
 2 BEFORE THE PATENT TRIAL AND APPEAL BOARD
 3
 4
 5 SYMANTEC CORPORATION;)
 6)
 7 Petitioner,)
 8)
 9 vs.) Case No.
 10) IPR2015-00372
 11 THE TRUSTEES OF COLUMBIA)
 12 UNIVERSITY IN THE CITY OF)
 13 NEW YORK;)
 14)
 15 Patent Owner.)
 16 _____)
 17
 18 VIDEOTAPED DEPOSITION of MICHAEL T.
 19 GOODRICH, Ph.D., taken on behalf of Defendants,
 20 at 840 Newport Center Drive, Suite 400, Newport
 21 Beach, California, at 9:05 a.m. and ending at
 22 6:09 p.m., Monday, August 24, 2015, reported by
 23 Lynda L. Fenn, CSR No. 12566, Certified
 24 Shorthand Reporter within and for the State of
 25 California, pursuant to notice.

Page 3

1 APPEARANCES:
 2 For the Plaintiff:
 3 FENWICK & WEST, LLP
 4 BY: DAVID D. SCHUMANN, ESQ.
 5 555 California Street, 12th Floor
 6 San Francisco, California 94104
 7 (415) 875-2321
 8 dschumann@fenwick.com
 9
 10 For the Defendants:
 11 IRELL & MANELLA, LLP
 12 BY: H. ANNITA ZHONG, ESQ.
 13 1800 Avenue of the Stars, Suite 900
 14 Los Angeles, California 90067-4276
 15 (310) 277-1010
 16 hzhong@irell.com
 17 Also Present:
 18 Fritz Sperberg, Videographer
 19
 20
 21
 22
 23
 24
 25

Page 4

1 I N D E X
 2 EXAMINATION BY: PAGE
 3 MS. ZHONG 6
 4
 5
 6
 7 E X H I B I T S
 8
 9 NUMBER DESCRIPTION PAGE
 10 Exhibit 2011 A seven-page, double-sided 32
 11 document entitled Windows 2000
 12 Security Event Descriptions
 13 (Part 1 of 2)
 14 Exhibit 2012 A 11-page, double-sided 32
 15 document entitled Windows 2000
 16 Security Event Descriptions
 17 (Part 2 of 2)
 18 Exhibit 2013 A seven-page, double-sided 32
 19 document entitled Security
 20 Event Descriptions
 21 Exhibit 2014 A five-page, double-sided 32
 22 document entitled Audit Policy
 23 Exhibit 2015 A 15-page, double-sided 233
 24 document entitled Introduction
 25 to Computer Security
 INFORMATION REQUESTED
 (None)
 INSTRUCTION NOT TO ANSWER
 (None)

Page 5

1 Newport Beach, California
 2 Monday, August 24, 2015
 3 9:05 a.m. - 6:09 p.m.
 4
 5
 6
 7 THE VIDEOGRAPHER: Good morning. My name is
 8 Fritz Sperberg. I'm a videographer with DTI. The court
 9 reporter is Lynda Fenn also with DTI at 20750 Ventura
 10 Boulevard, Suite 205, Woodland Hills, California.
 11 Today's date is August 24th, 2015. The time
 12 is now 9:05 a.m.
 13 Our location is 840 Newport Center Drive in
 14 Newport Beach, California.
 15 Counsel, please identify yourselves and state
 16 whom you represent.
 17 MS. ZHONG: This is Annita Zhong from Irell &
 18 Manella and I represent Columbia University.
 19 THE VIDEOGRAPHER: It's on the far side of the
 20 binder, David.
 21 MR. SCHUMANN: Right here.
 22 THE VIDEOGRAPHER: Thank you.
 23 MR. SCHUMANN: David Schumann for Symantec.
 24 THE VIDEOGRAPHER: The witness today is
 25 Michael T. Goodrich.

Page 6

1 Would the reporter please swear in the
 2 witness.
 3
 4 MICHAEL T. GOODRICH, Ph.D.,
 5 produced as a witness on behalf of the Defendants, and
 6 having been first duly sworn, was examined and testified
 7 as follows:
 8
 9 THE VIDEOGRAPHER: You may begin.
 10
 11 EXAMINATION
 12 BY MS. ZHONG:
 13 **Q Good morning, Dr. Goodrich. Have you been**
 14 **deposed before?**
 15 A Yes.
 16 **Q So you know the general procedures for**
 17 **deposition; correct?**
 18 A Yes.
 19 **Q Okay. Is there any reason why you can't**
 20 **testify truthfully today?**
 21 A No.
 22 **Q And is there any reason why you can't provide**
 23 **an accurate -- accurate answers today?**
 24 A No.
 25 **Q Okay. So I've placed in front of you Exhibits**

Page 7

1 **1001 through 1024 from IPR 2015, 000372 and 378.**
 2 A Thank you.
 3 **Q Okay. IPR 20 -- IPR2015 00372 and 378**
 4 **involved the '084 patents; correct?**
 5 A Yes, I believe that's correct.
 6 **Q Okay. And the '084 patent is entitled "System**
 7 **and methods for detecting intrusions in a computer**
 8 **system by monitoring operating system registry**
 9 **accesses"?**
 10 A Yes.
 11 **Q Okay. And you agree that what differentiates**
 12 **the '084 patent from prior art is it uses data obtained**
 13 **from monitoring registry accesses in anomaly detection?**
 14 MR. SCHUMANN: Object to form.
 15 THE WITNESS: I would not say that that's a
 16 fair characterization, no.
 17 MS. ZHONG: Okay.
 18 BY MS. ZHONG:
 19 **Q Let's turn to Exhibit 1003, paragraph 37, page**
 20 **17. And the first sentence of paragraph 37 reads, "The**
 21 **system and method described in the specification claim**
 22 **to be different from other systems because they use data**
 23 **obtained from monitoring registry accesses with anomaly**
 24 **detection."**
 25 **Did I read it correctly?**

Page 8

1 A Yes.
 2 **Q And you don't want to -- are you changing that**
 3 **sentence or statement?**
 4 A No.
 5 **Q Okay. So as written here as described by the**
 6 **'084 specification what differentiates the '084**
 7 **specification from other system is that they use data**
 8 **obtained from monitoring registry accesses with anomaly**
 9 **detection; correct?**
 10 A So what I am opining here is that the
 11 specification of the '084 patent is claiming to be
 12 different from other systems because it uses data
 13 obtained from monitoring registry access and uses that
 14 with anomaly detection.
 15 **Q Okay. So as described by the '084 patent**
 16 **what -- the inventors believe they're different from**
 17 **other system is they use data obtained from monitoring**
 18 **registry accesses with anomaly detection --**
 19 MR. SCHUMANN: Object --
 20 MS. ZHONG: Is that correct?
 21 MR. SCHUMANN: Object to form.
 22 THE WITNESS: I'm not sure of the state of
 23 mind of the inventors but it is true that the system
 24 method described in the specifications claimed to be
 25 different from other systems because it uses data

Page 9

1 obtained from monitoring registry accesses and uses
 2 anomaly detection.
 3 BY MS. ZHONG:
 4 **Q Okay. And it's not any kind of anomaly**
 5 **detection, it's anomaly detection to determine whether a**
 6 **registry access is anomalous; is that correct?**
 7 A The -- if you have like some specific -- so
 8 the way that I did my analysis was to do it based on the
 9 claims and then compare that to the prior art. So if
 10 you have some specific question with respect to claims.
 11 That question was a little too general for me to be able
 12 to answer just sitting here today.
 13 **Q Okay. Turn to Claim One, page 16.**
 14 A Okay.
 15 **Q So Claim One, Step C requires, "Analyzing**
 16 **features from a record of a process that accesses the**
 17 **operating system registry to detect the deviations from**
 18 **normal computer usage to determine whether the access to**
 19 **the operating system registry is an anomaly"; correct?**
 20 A Yes.
 21 **Q And to determine whether the access to the**
 22 **operating system registry is an anomaly is to**
 23 **determining whether an access to the registry -- to**
 24 **determine that the -- the anomaly related to the**
 25 **registry access; is that correct?**

1 A Could you restate the question, please?
2 **Q Okay. And Claim One, Step C, to determining**
3 **whether the access to the operating system registry is**
4 **an anomaly is to determine the anomaly regarding a**
5 **registry access; is that correct?**

6 A So I think that the claim -- the meaning of
7 the claim is just as it's written here that "To
8 determine that component of the limitation is to
9 determine whether the access to the operating system
10 registry is an anomaly." And I did my analysis in my
11 declaration based on that understanding.

12 **Q So it's regarding the determination anomaly**
13 **about an access to the registry; is that correct?**

14 A So it's regarding to determine whether the
15 access to the operating system registry is an anomaly.

16 **Q What's your interpretation of the access to**
17 **the operating system registry?**

18 A Plain meaning.

19 **Q And the plain meaning is?**

20 A To access the operating system registry. Just
21 the standard understanding of that.

22 **Q So is that the same as registry access?**

23 A I don't -- I don't see immediately here --
24 sitting here what the difference would be between reg --
25 what you're calling a registry access.

1 **Q Okay. So the access to the operating system**
2 **registry and registry access to you means the same**
3 **thing?**

4 A They may be the same thing. I did -- like I
5 said, I did my analysis using the exact words of the
6 claim limitation.

7 **Q So is there a difference between registry**
8 **access and the access to the operating system registry?**

9 A Just sitting here today, I'm not seeing
10 immediately what the difference would be but there may
11 be that I'm just overlooking at this point. Again, I
12 used the exact words from -- from the claim.

13 **Q Okay. And Step C requires a record of a**
14 **process that accessed the operating system registry.**

15 **Do you see that?**

16 A Yes.

17 **Q And a record of a process that accessed the**
18 **operating system registry refers to a registry access**
19 **record when you are dealing with a Windows system;**
20 **right?**

21 A The --

22 MR. SCHUMANN: Object to form.

23 THE WITNESS: As I mentioned in my declaration
24 that they -- in the prosecution history for this patent,
25 I believe there was a specific reference to the Windows

1 operating system that then was omitted from the claims
2 and that this is now referring generically to operating
3 system registry.

4 MS. ZHONG: Okay.

5 BY MS. ZHONG:

6 **Q So when this is applied to a Windows system,**
7 **is a record of a process that accessed the operating**
8 **system registry the same as a Window registry access**
9 **record?**

10 A Certainly that would be inclusive of that but
11 it could be potentially even broader because it doesn't
12 specifically call out on the claim the Microsoft Windows
13 Operating System.

14 **Q Okay. So when you were applying this to Bace,**
15 **Bace's event log, what are you applying the -- a record**
16 **of a process that accessed the operating system registry**
17 **to? What are you reading onto?**

18 A Right. So I discuss this in my declaration
19 with respect to the '084 patent. I gave a claim chart
20 as a part of this --

21 **Q Mm-hmm.**

22 A -- where I broke down each of these
23 components. And as I opine here, "Bace discloses
24 analyzing features from a record of processes -- of a
25 process that accesses the operating system registry to

1 detect deviations from normal computer usage to
2 determine whether the access to the operating system
3 registry is an anomaly. "For example," and then I have
4 a citation from Bace on performing analysis, "the second
5 of the three phases in the analyzer is the operational
6 analysis of a live event stream. In this phase the
7 analyzer is applied to live data to spot intrusions and
8 other activity of interest," dot, dot, dot.

9 **Q Okay.**

10 A The --

11 **Q So what I don't understand is after reading**
12 **this I'm still -- it's not clear to me what exactly you**
13 **are mapping onto.**

14 **Why don't we look at paragraph 88?**

15 A Okay. I'm there.

16 **Q And the last sentence is -- your opinion is,**
17 **"Because one of ordinary skill in the art would**
18 **understand that a Windows NT event logging would capture**
19 **registry data. All these references inherently suggest**
20 **using records of Windows registry accesses as**
21 **information source for intrusion detection methods."**

22 **Did I read it correctly?**

23 A Yes.

24 **Q Okay. So are you reading records of Windows**
25 **registry accesses as -- are you mapping records of**

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.