

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

**SYMANTEC CORPORATION**  
**Petitioner**

**v.**

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

---

**CASE IPR2015-00375**  
**Patent 8,074,115**

---

**DECLARATION OF GEORGE CYBENKO, Ph.D. IN SUPPORT OF  
COLUMBIA'S PATENT OWNER RESPONSE**

*Mail Stop "PATENT BOARD"*  
Patent Trial and Appeal Board  
U.S. Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
I. Introduction .....	1
II. Basis Of Opinion .....	1
A. Qualifications And Background.....	1
B. Materials Considered .....	3
III. Legal Standards .....	4
A. Standard Of Proof .....	4
B. Scope Of Prior Art .....	4
C. The Anticipation Inquiry.....	5
D. The Obviousness Inquiry .....	6
IV. Level Of Ordinary Skill In The Art.....	8
V. The Invention Of The '115 Patent.....	12
VI. Background On Symantec's Cited Prior Art.....	15
A. Khazan.....	15
1. Khazan Uses Static Analysis To Construct A Simple List Of Function Calls And Related Information .....	16
2. Khazan Uses Dynamic Analysis To Verify Function Calls .....	21
3. Khazan Distinguishes Itself From Anomaly Detection .....	23
4. Khazan Teaches Tracking Only Predetermined DLL Function Calls .....	24
B. Arnold.....	26
C. Agrawal .....	31

1.	Agrawal’s Detection Algorithms .....	31
2.	Agrawal’s Usage Of Its Detection Algorithms.....	35
3.	Many of Agrawal’s Models Are Statistical Models That Are Created Using Machine Learning .....	39
4.	Agrawal’s Markov Process Models.....	41
VII.	Ground 1: Khazan Does Not Anticipate Claims 22, 25, 27,-29, 32, 35-39 or 42 .....	43
A.	Khazan Does Not Disclose Identifying A Function Call As Anomalous .....	43
1.	Khazan Does Not Disclose “A Model of Typical Computer System Usage” .....	43
2.	Khazan Does Not Disclose Identifying A “Deviation From A Model” .....	46
B.	Khazan Does Not Disclose “Modifying A Program To Include Indicators Of Program-Level Function Calls” .....	52
1.	Khazan Does Not Teach That The Program Application Itself Is Modified .....	53
2.	Khazan Does Not Disclose Indicators Of Which Of The Program’s Internal Functions Are Being Called .....	58
C.	Khazan Does Not Disclose A “Model Of Function Calls” .....	60
D.	Khazan Does Not Disclose An “Emulator” .....	65
E.	Khazan Does Not Disclose “The Model Reflects Normal Activity” .....	75
F.	Khazan Does Not Disclose “The Model Reflects Attacks Against The At Least A Part Of The Program,” Nor Would It Be Obvious To Modify Khazan To Include This Limitation .....	77

VIII.	Ground 2: Claims 1, 4-8, 11, 14-18, 21, Or 26 Are Not Obvious Under The Combination Of Khazan And Arnold .....	79
A.	The Combination Of Khazan And Arnold Does Not Render Obvious An “Application Community” .....	79
B.	The Combination Of Khazan And Arnold Does Not Render Obvious “Upon Identifying The Anomalous Function Call,” Notifying Any Computer “Of The Anomalous Function Call” .....	84
IX.	Ground 3: Claims 2-3, 9-10, 12-13, 19-20, 23-24, 30-31, 33-34, Or 40-41 Are Not Obvious Under The Combination Of Khazan, Arnold, And Agrawal .....	93
A.	The Combination Of Khazan, Arnold, And Agrawal Does Not Disclose “Randomly Selecting The Model As To Be Used In The Comparison From A Plurality Of Different Models Relating To The Program” .....	93
1.	A Markov Process Model Is Not Random.....	93
2.	Agrawal Does Not Teach Using A Markov Model To Select Which Model Is Used.....	95
3.	A POSITA Would Not Have Modified Khazan To Incorporate Random Selection Of Models .....	97
4.	Dr. Goodrich’s New Arguments Raised For The First Time At Deposition Are Not Accurate .....	99
5.	Sobel Does Not Suggest Random Selection Of Models.....	103
B.	The Combination of Khazan, Arnold, and Agrawal Does Not Disclose “Randomly Selecting A Portion Of The Model To Be Used In The Comparison” .....	104
C.	The Combination Of Khazan, Arnold, And Agrawal Does Not Disclose “Creating A Combined Model From At Least Two Models Created Using Different Computers” .....	106

1.	Agrawal Does Not Render This Limitation Obvious .....	106
2.	A Combination Of Khazan, Arnold, and Agrawal Would Not Include The Limitation .....	109
D.	The Combination Of Khazan, Arnold, And Agrawal Does Not Disclose “Creating A Combined Model From At Least Two Models Created At Different Times” .....	111
1.	Agrawal Does Not Render This Limitation Obvious .....	111
2.	A Combination Of Khazan, Arnold, and Agrawal Would Not Include The Limitation .....	115
E.	Khazan, Arnold, and Agrawal May Not Be Combined to Render the Challenged Claims Obvious .....	118

# 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.