IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK, *Plaintiff* vs. SYMANTEC CORPORATION, *Defendant*	Civil Action No. 3:13-cv-00808-JRS **JURY TRIAL DEMANDED**

DECLARATION OF PROFESSOR DOUGLAS C. SZAJDA

TABLE OF CONTENTS

Page

I. Background and Qualifications

1. I am a professor with tenure in the Department of Mathematics and Computer Science at the University of Richmond. I received my PhD in Mathematics and a Masters of Computer Science from the University of Virginia in 1999. I then held a post-doctoral fellowship in Computer Science at the University of Maryland Institute for Advanced Computer Studies. Exhibit A is a copy of my CV. All exhibits in my declaration are in the Declaration of Gavin Snyder ("Snyder Decl.").

2. Several aspects of my professional life are relevant to the subject of this declaration. First, I train computer scientists in aspects of computer security directly relevant to the three families of Columbia patents that I understand are issue in this case. I teach Computer Networks and Computer Security classes in my department. In addition, under the auspices of programs such as the National Science Foundation Cyber Trust program grant, I train computer security researchers in the laboratory. These students conduct research at the top universities and technology companies in the country, including Microsoft and Google. I also have been the coordinator of the University of Richmond's System Security Group since 2002.

3. Second, outside of the University I have devoted a large portion of my professional life to issues of computer security. I served as General Chair of the Internet Society's Network and Distributed System Security ("NDSS") Symposium from 2008–2011, as an NDSS steering group member since 2007, and as a member of the conference organizing committee from 2005–2007. I have served on program committees for NDSS and the security track of the International Conference on Security Data Services. I have also reviewed papers for both the IEEE Symposium on Security and Privacy and the USENIX Security Symposium. These are some of the most prominent conferences on computer security in the world.

4. Third, the research group I lead at the University of Richmond is focused on applying the same type of technology described in the three patent families at issue in this case: using machine learning techniques based on artificial intelligence to detect whether web pages contain malicious programs (*e.g.*, via embedded scripts or through links that cause malicious scripts to be downloaded and executed). Indeed, we have a constructed a working platform that can perform real-time analysis of web pages to detect if they are hosting malicious programs. The platform has three parts: an instrumented web crawler for collecting candidate pages, an extraction unit to extract relevant features of the pages, and an analysis unit, which creates artificial intelligence models. The prototype is capable of mining virtually any data that is freely available over the Internet, and, with slight modification, can potentially perform analysis of any network transported malware.

II. Legal Standards Applied

5. Appendix A lists the legal standards I have been asked to apply in my analysis and discussion.

III. Subject of the Declaration and Basis for Opinions

6. I have been asked to provide background information on the technology in the three families of Columbia patents at issue in the case. As part of this process, I have also provided a summary of how a person of ordinary skill in the art of the patents would understand a number of the concepts that I understand are at issue in the proceedings. In preparing this declaration I have relied on my extensive experience in the field, as well the materials referenced in this declaration and certain material listed in Appendix B.

DOCKET ALARM

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.