

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

NINTENDO CO., LTD., and  
NINTENDO OF AMERICA INC.,  
Petitioners,

v.

MALIKIE INNOVATIONS LTD.,  
Patent Owner.

---

Case IPR2026-00007  
U.S. Patent No. 9,542,571 B2  
Issue Date: January 10, 2017

Title: SYSTEM AND METHOD OF OWNER APPLICATION CONTROL OF  
ELECTRONIC DEVICES

---

**DECLARATION OF NATHANIEL POLISH, PH.D. IN SUPPORT OF  
PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,542,571**

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

**TABLE OF CONTENTS**

|                                                                                                                                                                                     | <b>Page</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| I. INTRODUCTION .....                                                                                                                                                               | 12          |
| A. Qualifications .....                                                                                                                                                             | 12          |
| B. Materials Considered.....                                                                                                                                                        | 14          |
| II. PERSON OF ORDINARY SKILL IN THE ART (“POSITA”).....                                                                                                                             | 16          |
| III. STATEMENT OF LEGAL PRINCIPLES.....                                                                                                                                             | 18          |
| A. Claim Construction .....                                                                                                                                                         | 18          |
| B. Obviousness.....                                                                                                                                                                 | 20          |
| IV. THE ’571 PATENT (EX1001).....                                                                                                                                                   | 26          |
| A. Overview of the Specification.....                                                                                                                                               | 26          |
| B. Challenged Claims .....                                                                                                                                                          | 32          |
| V. APPLICATION OF THE PRIOR ART TO THE<br>CHALLENGED CLAIMS .....                                                                                                                   | 40          |
| A. Summary and Overview of Lambert Grounds Prior Art<br>(Grounds 1-2) .....                                                                                                         | 40          |
| 1. Lambert (EX1004) .....                                                                                                                                                           | 40          |
| 2. Frank (EX1005) .....                                                                                                                                                             | 49          |
| 3. Gomberg (EX1006).....                                                                                                                                                            | 51          |
| 4. Windows Guidelines Book (EX1010) .....                                                                                                                                           | 52          |
| B. Grounds 1-2: Claims 1-20 are Obvious Over Lambert<br>(Ground 1); Claims 1-20 are Obvious Over Lambert in View of<br>Frank, Gomberg, and Windows Guidelines Book (Ground 2) ..... | 55          |
| 1. Independent Claim 1 .....                                                                                                                                                        | 55          |
| (a) “A method of application control on an<br>electronic device, the method comprising:”<br>(Claim 1[p]) .....                                                                      | 55          |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                                                | <b>Page</b> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (b) “receiving, by the electronic device, owner information from an owner of the electronic device;” (Claim 1[a]) .....                                                                                                                                                        | 58          |
| (c) “receiving, by the electronic device, owner control information that comprises:” (Claim 1[b]) .....                                                                                                                                                                        | 67          |
| (d) “a list of applications permitted for installation on the electronic device, and” (Claim 1[b][i]).....                                                                                                                                                                     | 71          |
| (e) “permissions associated with each permitted application in the list of applications;” (Claim 1[b][ii]) .....                                                                                                                                                               | 79          |
| (f) “storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;” (Claim 1[c])..... | 83          |
| (g) “receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 1[d]).....                                                                                                | 93          |
| (h) “determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 1[e]) .....                                                               | 99          |
| (i) “controlling application access to the local memory based upon the determining.” (Claim 1[f]) ...                                                                                                                                                                          | 104         |
| 2. Dependent claim 2 .....                                                                                                                                                                                                                                                     | 109         |
| 3. Dependent claim 3 .....                                                                                                                                                                                                                                                     | 112         |
| 4. Dependent claim 4 .....                                                                                                                                                                                                                                                     | 113         |

## TABLE OF CONTENTS

|     |                                                                                                                                                                                                                                                                                           | <b>Page</b> |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 5.  | Dependent claim 5 .....                                                                                                                                                                                                                                                                   | 114         |
| 6.  | Dependent claim 6 .....                                                                                                                                                                                                                                                                   | 120         |
| 7.  | Dependent claim 7 .....                                                                                                                                                                                                                                                                   | 122         |
| 8.  | Dependent claim 8 .....                                                                                                                                                                                                                                                                   | 124         |
|     | (a) “The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:” (Claim 8[p]) .....                                                                   | 124         |
|     | (b) “receiving requests to access the local memory from a plurality of applications operating on the electronic device;” (Claim 8[a]) .....                                                                                                                                               | 125         |
|     | (c) “determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and:” (Claim 8[b]) ..... | 126         |
|     | (d) “controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.” (Claim 8[c]) .....                                                                                                                                    | 127         |
| 9.  | Dependent claim 9 .....                                                                                                                                                                                                                                                                   | 127         |
| 10. | Independent claim 10 .....                                                                                                                                                                                                                                                                | 130         |
|     | (a) “A device, comprising:” (Claim 10[p]) .....                                                                                                                                                                                                                                           | 130         |
|     | (b) “a memory; and” (Claim 10[a]) .....                                                                                                                                                                                                                                                   | 132         |
|     | (c) “a processor coupled with the memory and configured by instructions stored in the memory to:” (Claim 10[b]) .....                                                                                                                                                                     | 133         |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                         | <b>Page</b> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (d) “receive owner information from an owner of the device;” (Claim 10[b][i]) .....                                                                                                                                                                     | 135         |
| (e) “receive owner control information that comprises;” (Claim 10[b][ii]) .....                                                                                                                                                                         | 135         |
| (f) “a list of applications permitted for installation on the device, and” (Claim 10[b][ii][A]) .....                                                                                                                                                   | 135         |
| (g) “permissions associated with each permitted application in the list of applications;” (Claim 10[b][ii][B]) .....                                                                                                                                    | 135         |
| (h) “store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information” (Claim 10[b][iii]) ..... | 136         |
| (i) “receive, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 10[b][iv]) .....                                                                                               | 136         |
| (j) “determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 10[b][v]) .....                                      | 136         |
| (k) “control application access to the local memory based upon the determining.” (Claim 10[b][vi]) .....                                                                                                                                                | 136         |
| 11. Dependent claim 11 .....                                                                                                                                                                                                                            | 136         |
| 12. Dependent claim 12 .....                                                                                                                                                                                                                            | 137         |
| 13. Dependent claim 13 .....                                                                                                                                                                                                                            | 137         |
| 14. Dependent claim 14 .....                                                                                                                                                                                                                            | 139         |
| 15. Dependent claim 15 .....                                                                                                                                                                                                                            | 139         |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                      | <b>Page</b> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 16. Dependent claim 16 .....                                                                                                                                                                                                                         | 140         |
| 17. Independent claim 17 .....                                                                                                                                                                                                                       | 140         |
| (a) “A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:” (Claim 17[p]) .....                                    | 140         |
| (b) “receiving owner information from an owner of an electronic device;” (Claim 17[a]) .....                                                                                                                                                         | 142         |
| (c) “receiving owner control information that comprises:” (Claim 17[b]) .....                                                                                                                                                                        | 143         |
| (d) “a list of applications permitted for installation on the device, and” (Claim 17[b][i]) .....                                                                                                                                                    | 143         |
| (e) “permissions associated with each permitted application in the list of applications;” (Claim 17[b][ii]) .....                                                                                                                                    | 143         |
| (f) “storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;” (Claim 17[c])..... | 144         |
| (g) “receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 17[d]) .....                                                                                              | 144         |
| (h) “determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 17[e]) .....                                    | 144         |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                                                                          | <b>Page</b> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (i) “controlling application access to the local<br>memory based upon the determining.” (Claim<br>17[f]) .....                                                                                                                                                                                           | 145         |
| 18. Dependent claim 18 .....                                                                                                                                                                                                                                                                             | 145         |
| 19. Dependent claim 19 .....                                                                                                                                                                                                                                                                             | 148         |
| 20. Dependent claim 20 .....                                                                                                                                                                                                                                                                             | 148         |
| C. Summary and Overview of Hayes-Grounds Prior Art (Grounds<br>3-5) .....                                                                                                                                                                                                                                | 149         |
| 1. Hayes (EX1011).....                                                                                                                                                                                                                                                                                   | 149         |
| 2. Sprigg (EX1012).....                                                                                                                                                                                                                                                                                  | 153         |
| 3. Frank (EX1005) .....                                                                                                                                                                                                                                                                                  | 156         |
| 4. Guedalia (EX1013) .....                                                                                                                                                                                                                                                                               | 157         |
| 5. Lambert (EX1004) .....                                                                                                                                                                                                                                                                                | 158         |
| D. Grounds 3-5: Claims 1-8 and 10-20 Are Obvious Over Hayes<br>in view of Sprigg (Ground 3); Claims 1-8 and 10-20 Are<br>Obvious Over Hayes in view of Sprigg, Frank, and Guedalia<br>(Ground 4); Claims 9-20 Are Obvious Over Hayes in view of<br>Sprigg, Frank, Guedalia, and Lambert (Ground 5) ..... | 158         |
| 1. Independent Claim 1 .....                                                                                                                                                                                                                                                                             | 158         |
| (a) “A method of application control on an electronic<br>device, the method comprising:” (Claim 1[p]).....                                                                                                                                                                                               | 158         |
| (b) “receiving, by the electronic device, owner<br>information from an owner of the electronic<br>device;” (Claim 1[a]) .....                                                                                                                                                                            | 159         |
| (c) “receiving, by the electronic device, owner control<br>information that comprises:” (Claim 1[b]) and “a<br>list of applications permitted for installation on the<br>electronic device, and” (Claim 1[b][i]) .....                                                                                   | 164         |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                                                | <b>Page</b> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (d) “permissions associated with each permitted application in the list of applications;” (Claim 1[b][ii]) .....                                                                                                                                                               | 174         |
| (e) “storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;” (Claim 1[c])..... | 189         |
| (f) “receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 1[d]).....                                                                                                | 192         |
| (g) “determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 1[e]) .....                                                               | 194         |
| (h) “controlling application access to the local memory based upon the determining.” (Claim 1[f]) ...                                                                                                                                                                          | 197         |
| 2. Dependent claim 2 .....                                                                                                                                                                                                                                                     | 199         |
| 3. Dependent claim 3 .....                                                                                                                                                                                                                                                     | 200         |
| 4. Dependent claim 4 .....                                                                                                                                                                                                                                                     | 201         |
| 5. Dependent claim 5 .....                                                                                                                                                                                                                                                     | 203         |
| 6. Dependent claim 6 .....                                                                                                                                                                                                                                                     | 210         |
| 7. Dependent claim 7 .....                                                                                                                                                                                                                                                     | 212         |
| 8. Dependent claim 8 .....                                                                                                                                                                                                                                                     | 214         |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                                                           | <b>Page</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (a) “The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:” (Claim 8[p]) .....                                                                   | 214         |
| (b) “receiving requests to access the local memory from a plurality of applications operating on the electronic device;” (Claim 8[a]) .....                                                                                                                                               | 220         |
| (c) “determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and:” (Claim 8[b]) ..... | 221         |
| (d) “controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.” (Claim 8[c]) .....                                                                                                                                    | 222         |
| 9. Dependent claim 9 .....                                                                                                                                                                                                                                                                | 223         |
| 10. Independent claim 10 .....                                                                                                                                                                                                                                                            | 230         |
| (a) “A device, comprising:” (Claim 10[p]) .....                                                                                                                                                                                                                                           | 230         |
| (b) “a memory; and” (Claim 10[a]) .....                                                                                                                                                                                                                                                   | 231         |
| (c) “a processor coupled with the memory and configured by instructions stored in the memory to:” (Claim 10[b]) .....                                                                                                                                                                     | 235         |
| (d) “receive owner information from an owner of the device;” (Claim 10[b][i]) .....                                                                                                                                                                                                       | 237         |
| (e) “receive owner control information that comprises:” (Claim 10[b][ii]) .....                                                                                                                                                                                                           | 238         |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                         | <b>Page</b> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (f) “a list of applications permitted for installation on the device, and” (Claim 10[b][ii][A]).....                                                                                                                                                    | 238         |
| (g) “permissions associated with each permitted application in the list of applications,” (Claim 10[b][ii][B]) .....                                                                                                                                    | 238         |
| (h) “store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information” (Claim 10[b][iii]) ..... | 238         |
| (i) “receive, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 10[b][iv]) .....                                                                                               | 239         |
| (j) “determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 10[b][v]) .....                                      | 239         |
| (k) “control application access to the local memory based upon the determining.” (Claim 10[b][vi]) .....                                                                                                                                                | 239         |
| 11. Dependent claim 11 .....                                                                                                                                                                                                                            | 239         |
| 12. Dependent claim 12 .....                                                                                                                                                                                                                            | 240         |
| 13. Dependent claim 13 .....                                                                                                                                                                                                                            | 240         |
| 14. Dependent claim 14 .....                                                                                                                                                                                                                            | 242         |
| 15. Dependent claim 15 .....                                                                                                                                                                                                                            | 243         |
| 16. Dependent claim 16 .....                                                                                                                                                                                                                            | 243         |
| 17. Independent claim 17 .....                                                                                                                                                                                                                          | 244         |

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                       | <b>Page</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (a) “A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:” (Claim 17[p]) .....                                     | 244         |
| (b) “receiving owner information from an owner of an electronic device;” (Claim 17[a]) .....                                                                                                                                                          | 246         |
| (c) “receiving owner control information that comprises:” (Claim 17[b]) .....                                                                                                                                                                         | 246         |
| (d) “a list of applications permitted for installation on the device, and” (Claim 17[b][i]) .....                                                                                                                                                     | 247         |
| (e) “permissions associated with each permitted application in the list of applications;” (Claim 17[b][ii]) .....                                                                                                                                     | 247         |
| (f) “storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;” (Claim 17[c]) ..... | 247         |
| (g) “receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 17[d]) .....                                                                                               | 247         |
| (h) “determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 17[e]) .....                                     | 248         |
| (i) “controlling application access to the local memory based upon the determining.” (Claim 17[f]) .....                                                                                                                                              | 248         |

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

**TABLE OF CONTENTS**

|                                                        | <b>Page</b> |
|--------------------------------------------------------|-------------|
| 18. Dependent claim 18 .....                           | 248         |
| 19. Dependent claim 19 .....                           | 254         |
| 20. Dependent claim 20 .....                           | 254         |
| VI. NO SECONDARY CONSIDERATIONS OF NONOBVIOUSNESS..... | 255         |
| VII. CONCLUSION.....                                   | 255         |

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

I, Nathaniel Polish, Ph.D., declare as follows:

**I. INTRODUCTION**

1. I prepared this declaration as an expert on behalf of Petitioner Nintendo Co., Ltd., and Nintendo of America Inc. (“Petitioner”).

2. I provide my opinions in this declaration regarding the invalidity of claims 1-20 of U.S. Patent No. 9,542,571 B2 (the “’571 patent”) (**EX1001**).

**A. Qualifications**

3. My qualifications are set forth in my curriculum vitae (**Appendix A**).<sup>1</sup>

4. I have a Ph.D. in Computer Science from Columbia University. I hold the following degrees from Columbia, spanning the years 1980 to 1993:

- Ph.D. in Computer Science, May 1993;
- M.Phil. in Computer Science, December 1989;
- M.S. in Computer Science, December 1987; and
- B.A. in Physics, Columbia College, May 1984.

5. For over thirty years, I have run a computer technology development firm that I co-founded, called Daedalus Technology Group. I develop hardware and

---

<sup>1</sup> Appendix A includes a list of my publications and a list of cases in which I have testified during the last five years.

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

software as well as supervise others who do so. My business involves understanding the business objectives of customers, designing products to suit their needs, and supervising the building, testing, and deployment of products.

6. I am very familiar with and experienced in the field of the '571 patent. Through the 1990s and mid-2010s, I designed and implemented many large collections of servers to support my clients' products. These included systems with permission structures. One system in particular for a client called Assurenet involved many dozens of Linux computers running virtual windows computers loaded with insurance company illustration applications.

7. One of my current firms, SuperAlert, uses a distributed network of sensor computers, data collection computers, and data presentation computers. These systems need to maintain security and permission structures to keep data and applications from different SuperAlert customers properly separated.

8. I have used many different systems to manage and maintain collections of computers over the years. For example, the many server and client computer systems my firms and I have built over the years managed which applications were loaded on to different categories of computers.

9. From time to time, I have started other companies in order to pursue particular product opportunities. Most of my business activity, however, is as a

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

consulting product developer. From time to time, I have also served as an expert witness on computer and software-related cases, which are listed in my CV.

**B. Materials Considered**

10. My opinions in this declaration are based on my professional and academic experience, as well as documents I have considered. In forming my opinions, I have read and considered U.S. Patent No. 9,542,571 B2 (**EX1001**) and its prosecution history (**EX1003**). The following documents are cited in this declaration:

| <b>Exhibit No.</b> | <b>Description of Document</b>                                                                                                                                                                                    |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1001</b>        | U.S. Patent No. 9,542,571 B2 to Neil P. Adams, et al. (filed May 18, 2015, issued January 10, 2017) (“’571” or “’571 patent”)                                                                                     |
| <b>1002</b>        | Declaration of Nathaniel Polish, Ph.D. (“Polish”)                                                                                                                                                                 |
| <b>1003</b>        | Prosecution history of U.S. Patent No. 9,542,571 (Parts 1 and 2)                                                                                                                                                  |
| <b>1004</b>        | U.S. Patent Application No. 2002/0099952 A1 (filed June 8, 2001, published July 25, 2002) (“Lambert”)                                                                                                             |
| <b>1005</b>        | U.S. Patent Application No. 2002/0095572 A1 (filed January 12, 2001, published July 18, 2002) (“Frank”)                                                                                                           |
| <b>1006</b>        | Gomberg, M., Evard, R., and Stacey, C., “A Comparison of Large-Scale Software Installation Methods on NT and UNIX,” <i>Mathematics and Computer Science Division, Argonne National Laboratory</i> , USENIX (1998) |
| <b>1007</b>        | Declaration of Ingrid Hsieh-Yee, Ph.D.                                                                                                                                                                            |

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

| <b>Exhibit No.</b> | <b>Description of Document</b>                                                                                                                                                                                                           |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1008</b>        | Argonne National Laboratory webpage, <i>About Argonne</i> , available at <a href="https://www.anl.gov/argonne-national-laboratory">https://www.anl.gov/argonne-national-laboratory</a>                                                   |
| <b>1009</b>        | Department of Energy webpage, <i>Argonne National Laboratory</i> , available at <a href="https://www.energy.gov/ea/argonne-national-laboratory">https://www.energy.gov/ea/argonne-national-laboratory</a>                                |
| <b>1010</b>        | <i>The Windows Interface Guidelines for Software Design</i> , Microsoft Corporation, pp. xvii-xviii, 272-275 (1995) (“Windows Guidelines Book”)                                                                                          |
| <b>1011</b>        | U.S. Patent Application No. 2001/0011341 A1 (filed May 5, 1998, published August 2, 2001) (“Hayes”)                                                                                                                                      |
| <b>1012</b>        | U.S. Patent No. 7,743,407 B2 to Stephen A. Sprigg and Laurence Lundblade (filed August 13, 2002, issued June 22, 2010) (“Sprigg”)                                                                                                        |
| <b>1013</b>        | U.S. Patent No. 6,121,970 to Joshua Siegfried Guedalia (filed November 26, 1997, issued September 19, 2000) (“Guedalia”)                                                                                                                 |
| <b>1014</b>        | Kumar, S. Rajesh and Aravazhi, R., “A Study on Ajax in Web Applications with Latest Trends,” <i>International Journal on Recent and Innovation Trends in Computing and Communication</i> , Vol. 1, Issue 6, pp. 563-568 (2013) (“Kumar”) |
| <b>1015</b>        | Spencer, Donald D., <i>Spencer’s Illustrated Computer Dictionary</i> , Camelot Publishing Co., p. 231 (1995)                                                                                                                             |
| <b>1016</b>        | K.F. Ibrahim, <i>Electronic Systems &amp; Techniques</i> , <u>2nd Edition</u> , p. 66 (1994)                                                                                                                                             |
| <b>1017</b>        | <i>Microsoft Computer Dictionary</i> , Microsoft Press, 5th Edition, pp. 94, 196, 254, 440, 445, 446, 572, 575 (2002)                                                                                                                    |

11. For my efforts in connection with the preparation of this declaration, I am being compensated at my usual and customary rate of \$750/hr. My

compensation is in no way contingent on the results of these or any other proceedings (or any issue in these or any other proceedings) related to the '571 patent or any other patent.

12. This declaration discloses my opinions formed to date and my bases and rationale for those opinions. I reserve the right to offer further opinions based on ongoing review of materials, including opinions and/or testimony of other expert witnesses.

## **II. PERSON OF ORDINARY SKILL IN THE ART (“POSITA”)**

13. I understand that, under the patent laws in effect before the America Invents Act (“AIA”) of 2011, an assessment of claims of a patent filed before the AIA took effect should be undertaken from the perspective of a person of ordinary skill in the art (“POSITA”) as of the earliest claimed priority date (i.e., the “time the invention was made”). I have preliminarily for purposes of my declaration only assumed that date to be December 12, 2002, the earliest patent application to which the '571 patent claims priority.<sup>2</sup>

---

<sup>2</sup> I understand that in the pending litigation, the Patent Owner has claimed that the '571 patent is entitled to an invention date of December 2002. I express no opinion on whether the '571 patent is entitled to such an invention date.

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

14. I have also been advised that to determine the appropriate level of a person having ordinary skill in the art, the following factors may be considered: (1) the types of problems encountered by those working in the field and prior art solutions thereto; (2) the sophistication of the technology in question, and the rapidity with which innovations occur in the field; (3) the educational level of active workers in the field; and (4) the educational level of the inventor.

15. For purposes of assessing the level of skill necessary to understand the technology disclosed in the '571 patent, and based on my experience, it is my opinion that a POSITA at the time of the alleged invention of the '571 patent would have possessed a Bachelor's degree in software engineering, electrical engineering, or a similar degree, with two to three years of practical experience designing computer systems. A person could also have qualified as a POSITA with a combination of (1) more formal education and less technical experience, or (2) less formal education and more technical or professional experience.

16. Although my qualifications and experience exceed those of the hypothetical person having ordinary skill in the art defined above, my analysis and opinions regarding the '571 patent have been based on the perspective of a person of ordinary skill in the art as of December 2002.

17. The analysis and opinions in my declaration would not change if a

somewhat different POSITA definition (e.g., with less or more academic or professional experience) were applied.

### **III. STATEMENT OF LEGAL PRINCIPLES**

#### **A. Claim Construction**

18. I understand that a purpose of claim construction is to determine what a person of ordinary skill in the art would have understood the claim terms to mean. Claim terms are generally given their ordinary and customary meaning, which is the meaning that the term would have to a person of ordinary skill in the art in question as of the effective filing date.

19. I understand that the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. I understand that the patent specification, under the legal principles, has been described as the single best guide to the meaning of a claim term, and is thus highly relevant to the interpretation of claim terms. And I understand for terms that do not have a customary meaning within the art, the specification usually supplies the best context of understanding the meaning of those terms.

20. I further understand that other claims of the patent in question, both asserted and unasserted, can be valuable sources of information as to the meaning of

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

a claim term. Because the claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims. Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.

21. I understand that the prosecution history can further inform the meaning of the claim language by demonstrating how the inventors understood the invention and whether the inventors limited the invention in the course of prosecution, making the claim scope narrower than it otherwise would be. Extrinsic evidence, such as dictionaries, may also be consulted in construing the claim terms.

22. I understand that, in *Inter Partes* Review (“IPR”) proceedings, a claim of a patent shall be construed using the same claim construction standard that would be used to construe the claim in a civil action filed in a U.S. district court (which I understand is called the “*Phillips*” claim construction standard), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

23. I have been instructed by counsel to apply the “*Phillips*” claim construction standard for purposes of interpreting the claims in this proceeding, to the extent they require an explicit construction. The description of the legal

principles set forth above thus provides my understanding of the “*Phillips*” standard as provided to me by counsel.

24. I understand that certain terms appearing in the challenged claims have been the subject of dispute in the district court litigation. For purposes of my analysis here, I do not believe express claim constructions are necessary because the prior art renders the claim obvious under the claim constructions proposed by either party in the district court litigation.

**B. Obviousness**

25. I understand that a patent claim is obvious if, as of the effective filing date, it would have been obvious to a person having ordinary skill in the field of the technology (the “art”) to which the claimed subject matter belongs.

26. I understand that the following factors should be considered in analyzing obviousness: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; and (3) the level of ordinary skill in the pertinent art. I also understand that certain other facts known as “secondary considerations” such as commercial success, unexplained results, long felt but unsolved need, industry acclaim, simultaneous invention, copying by others, skepticism by experts in the field, and failure of others may be utilized as indicia of nonobviousness. I understand, however, that secondary considerations should be connected, or have a

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

“nexus,” with the invention claimed in the patent at issue.

27. I understand that a reference qualifies as prior art for obviousness purposes when it is analogous to the claimed invention. The test for determining what art is analogous is: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor’s endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.

28. I understand that a person of ordinary skill in the art is assumed to have knowledge of all prior art. I understand that one skilled in the art can combine various prior art references based on the teachings of those prior art references, the general knowledge present in the art, or common sense. I understand that a motivation to combine references may be implicit in the prior art, and there is no requirement that there be an actual or explicit teaching to combine two references. Thus, one may take into account the inferences and creative steps that a person of ordinary skill in the art would employ to combine the known elements in the prior art in the manner claimed by the patent at issue. I understand that one should avoid “hindsight bias” and ex post reasoning in performing an obviousness analysis. But this does not mean that a person of ordinary skill in the art for purposes of the obviousness inquiry does not have recourse to common sense.

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

29. I understand that when determining whether a patent claim is obvious in light of the prior art, neither the particular motivation for the patent nor the stated purpose of the patentee is controlling. The primary inquiry has to do with the objective reach of the claims, and that if those claims extend to something that is obvious, then the entire patent claim is invalid.

30. I understand one way that a patent can be found obvious is if there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. I understand that a motivation to combine various prior art references to solve a particular problem may come from a variety of sources, including market demand or scientific literature. I understand that a need or problem known in the field at the time of the invention can also provide a reason to combine prior art references and render a patent claim invalid for obviousness. I understand that familiar items may have obvious uses beyond their primary purpose, and that a person of ordinary skill in the art will be able to fit the teachings of multiple prior art references together like the pieces of a puzzle. I understand that a person of ordinary skill is also a person of at least ordinary creativity. I understand when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

technical grasp. If this finite number of predictable solutions leads to the anticipated success, I understand that the invention is likely the product of ordinary skill and common sense, and not of any sort of innovation. I understand that the fact that a combination was obvious to try might also show that it was obvious, and hence invalid, under the patent laws. I understand that if a patent claims a combination of familiar elements according to known methods, the combination is likely to be obvious when it does no more than yield predictable results. Thus, if a person of ordinary skill in the art can implement a predictable variation, an invention is likely obvious. I understand that combining embodiments disclosed near each other in a prior art reference would not ordinarily require a leap of inventiveness.

31. I understand that obviousness may be shown by demonstrating that it would have been obvious to modify what is taught in a single piece of prior art to create the patented invention. Obviousness may also be shown by demonstrating that it would have been obvious to combine the teachings of more than one item of prior art. I understand that a claimed invention may be obvious if some teaching, suggestion, or motivation exists that would have led a person of ordinary skill in the art to combine the invalidating references. I also understand that this suggestion or motivation may come from the knowledge of a person having ordinary skill in the art, or from sources such as explicit statements in the prior art. I understand that

when there is a design need or market pressure, and there are a finite number of predictable solutions, a person of ordinary skill may be motivated to apply common sense and his skill to combine the known options in order to solve the problem.

32. I understand the following are examples of approaches and rationales that may be considered in determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of a person having ordinary skill in the art:

- (1) Some teaching, motivation, or suggestion in the prior art that would have led a person of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;
- (2) Known work in one field of endeavor may prompt variations of it for use in the same field or a different field based on design incentives or other market forces if the variations would have been predictable to a person of ordinary skill in the art;
- (3) Combining prior art elements according to known methods to yield predictable results;
- (4) Applying a known technique to a known device, method, or product ready for improvement to yield predictable results;

- (5) Applying a technique or approach that would have been “obvious to try” (choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);
- (6) Simple substitution of one known element for another to obtain predictable results; or
- (7) Use of a known technique to improve similar products, devices, or methods in the same way.

33. I understand that, when determining whether a claimed combination is obvious, the correct analysis is not whether one of ordinary skill in the art, writing on a blank slate, would have chosen the particular combination of elements described in the claim. Instead, I understand the correct analysis considers whether one of ordinary skill, facing the wide range of needs created by developments in the field of endeavor, would have seen a benefit to selecting the combination claimed.

34. I understand that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. The test for obviousness, in other words, is not whether the references could be physically combined but whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole.

#### **IV. THE '571 PATENT (EX1001)**

##### **A. Overview of the Specification**

35. The title of the '571 patent is: "System and Method of Owner Application Control of Electronic Devices." ('571, Title.) The '571 patent states that the "system relates generally to electronic devices, and in particular to controlling application installation of such devices by a device owner." (*Id.*, 1:41-43.) The patent asserts that "[i]n a corporate environment, employees are often provided with access to office supplies and equipment to be used in performing job functions .... Although such equipment is intended primarily for business or work-related purposes, users sometimes make personal use of office equipment." (*Id.*, 1:44-51.) "In these types of situations, a user of an electronic device is not the owner of the device, and the user and owner may have different perceptions of acceptable device uses." (*Id.*, 1:56-58.)

36. Before the '571 patent, techniques for controlling operation of electronic devices in a business or work-related environment existed. For example, in one known technique, "an owner loads a policy file onto a device to restrict the type of operations or software applications that may be executed by the device." ('571, 1:63-67.) A user, however, may circumvent restrictions by "deleting the owner policy file or replacing the owner policy file with a user policy file which may

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

include fewer restrictions.” (*Id.*, 1:67-2:4.)

37. The '571 patent is aimed at “owner control”. Figure 3 depicts boxes: “a mobile device **30** comprises a memory **32**, a processor **40**, an application loader **42**, an insertion module **44**, a user interface (UI) **46**, a wireless transceiver **48**, and an interface/connector **50**.” ('571, 7:13-17.)

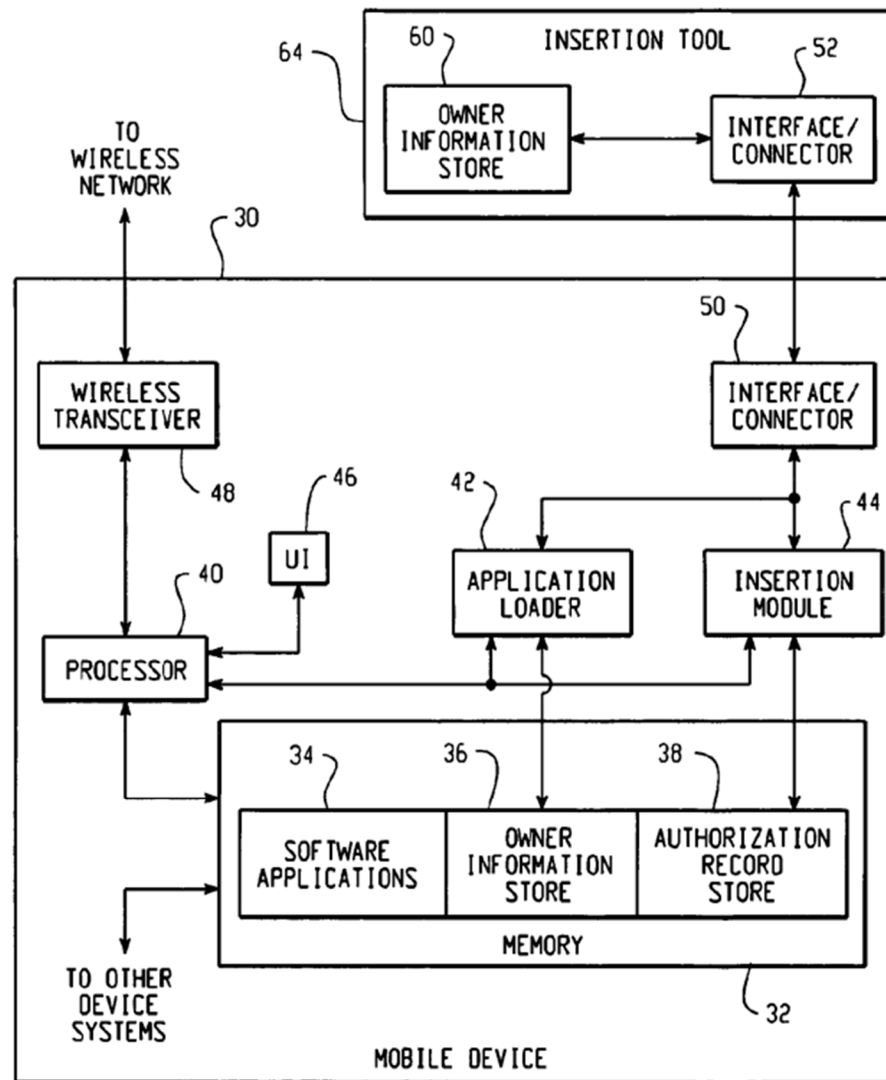


Fig. 3

(*Id.*, Fig. 3.) As explained below, this set-up preexisted the '571 patent. “The software application store 34 includes software applications that have been installed on the mobile device 30.” (*Id.*, 7:30-32.) “The owner information store 36 stores information such as an owner name or other identification, data integrity and

source authentication information, such as a digital signature public key associated with a digital signature private key of the owner.” (*Id.*, 7:35-39.) A digital signature public or private key is information. “Owner control information, in which an owner of the mobile device **30** specifies usage permissions and restrictions for the mobile device **30**, is stored in an authorization record in the authorization record store **38**.” (*Id.*, 7:39-43.)

38. Figure 6 is a simple flow diagram. Generally, the process involves receiving an operation request, checking for owner information, checking for owner control information, and using the information to determine whether the operation is permitted. (’571, 21:50-22:17.)

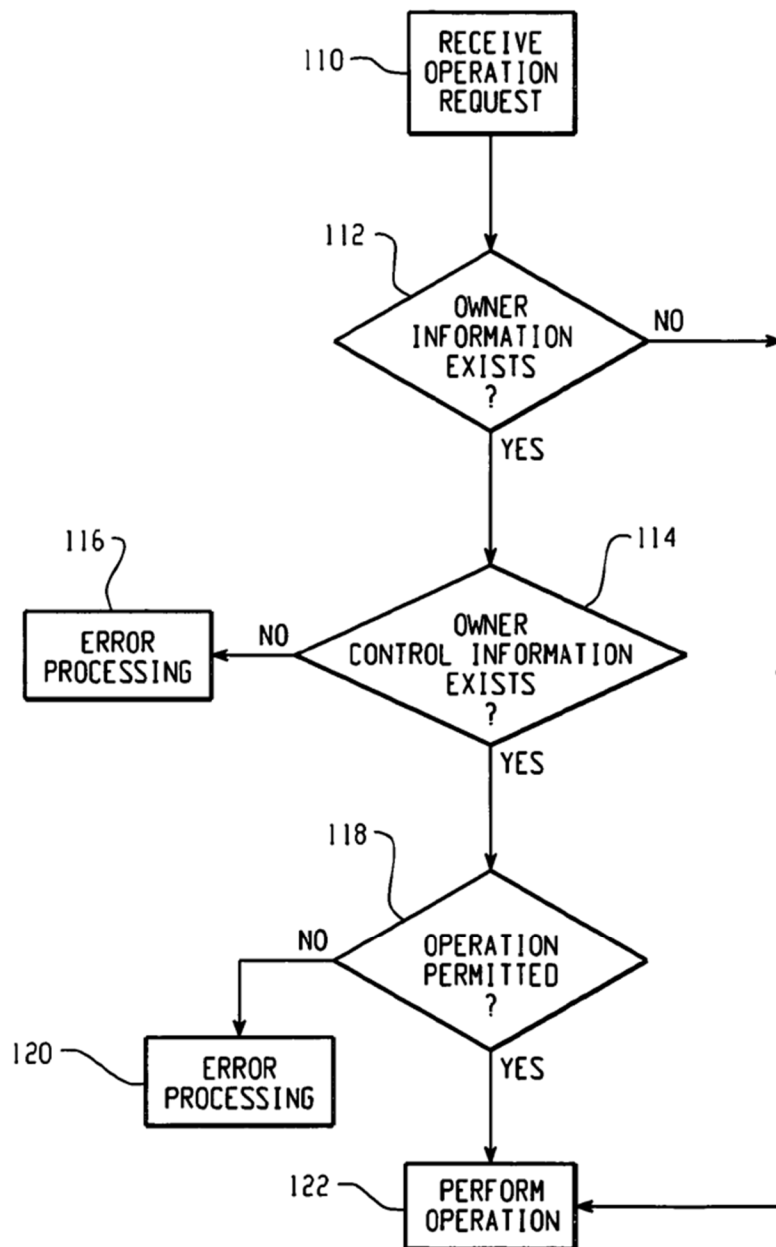


*Fig. 6*

(*Id.*, Fig. 6.) This is operating like a rule.

39. Owner information is “information, such as an owner name or other

identification information, for example, which identifies an owner of the electronic device **210**.” (’571, 5:25-28.) The ’571 patent discloses that owner information can be information provided by an administrator of a network of computers—*e.g.*, in a corporate network setting. (*Id.*, 5:63-67 (“Where the electronic device **210** is provided to a user by an employer, for example, the owner control insertion point **220** may be a computer system or device controlled by a corporate computer system administrator or IT department.”) (emphasis added), 6:44-50 (“In a large company, for example, corporate computer system administrators may be authorized to perform owner information insertion operations from administrator computer systems, or from any corporate computer system from which administrative functions can be accessed, thereby providing multiple owner information insertion points **220**.”) (emphasis added), 11:37-40, 19:14-17, 9:11-17, 8:7-10, 10:58-62.)

40. Owner control information “can include one or more applications lists”—for example, “application lists [that] provide owner control of application installation and deletion on the electronic device.” (’571, 4:34-56.) Such application lists may include allowable applications—*i.e.*, “applications may or may not be present on a device,” where “the user is free to download these applications if they desire the functionality that the application provides.” (*Id.*, 4:48-52.) Owner control information can also include permissions or restrictions on operation of the device.

“[O]peration controls can determine whether an application can connect to external resources, and if so, the channels (that may be used for such connections) can communicate with other applications executing on the device and/or can access part or all of local memory on the device.” (*Id.*, 14:28-39.)

**B. Challenged Claims**

41. Claims 1-20 (the “challenged claims”) of the ’571 patent are addressed in this declaration. Independent claim 1 recites:

1. A method of application control on an electronic device, the method comprising:
  - [a] receiving, by the electronic device, owner information from an owner of the electronic device;
  - [b] receiving, by the electronic device, owner control information that comprises:
    - [b][i] a list of applications permitted for installation on the electronic device, and
    - [b][ii] permissions associated with each permitted application in the list of applications;
  - [c] storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

- [d] receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;
- [e] determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and
- [f] controlling application access to the local memory based upon the determining.

(’571, 29:6-29 (Claim 1; bracketed notation (*e.g.*, [a]) added).)

42. Claim 2 recites:

- 2. The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

(’571, 29:30-32 (Claim 2).)

43. Claim 3 recites:

- 3. The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

(’571, 29:33-35 (Claim 3).)

44. Claim 4 recites:

- 4. The method of claim 1, further comprising restricting modification of the owner control information after the owner

control information has been stored in the protected data store.

(’571, 29:36-39 (Claim 4).)

45. Claim 5 recites:

5. The method of claim 1, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and the owner control information is provided by an external source through a wireless communication channel.

(’571, 29:40-44 (Claim 5).)

46. Claim 6 recites:

6. The method of claim 5, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

(’571, 29:45-49 (Claim 6).)

47. Claim 7 recites:

7. The method of claim 1, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

(’571, 29:50-52 (Claim 7).)

48. Claim 8 recites:

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

8. The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:
- [a] receiving requests to access the local memory from a plurality of applications operating on the electronic device;
  - [b] determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and
  - [c] controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.

(’571, 29:53-67 (Claim 8; bracketed notation (*e.g.*, [a]) added).)

49. Claim 9 recites:

9. The method of claim 8, wherein a group containing two or more of the applications is associated with one of the authorization records.

(’571, 30:1-3 (Claim 9).)

50. Independent claim 10 recites:

10. A device, comprising:

- [a] a memory; and

**[b]** a processor coupled with the memory and configured by instructions stored in the memory to:

**[b][i]** receive owner information from an owner of the device;

**[b][ii]** receive owner control information that comprises:

**[b][ii][A]** a list of applications permitted for installation on the device, and

**[b][ii][B]** permissions associated with each permitted application in the list of applications;

**[b][iii]** store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;

**[b][iv]** receive, from an application operating on the electronic device, a request to access local memory on the electronic device;

**[b][v]** determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and

**[b][vi]** control application access to the local memory based upon the determining.

(’571, 30:4-28 (Claim 10; bracketed notation (*e.g.*, **[a]**) added).)

51. Claim 11 recites:

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

11. The device of claim 10, wherein the request to access the local memory comprises a request to erase data from the local memory.

('571, 30:29-31 (Claim 11).)

52. Claim 12 recites:

12. The device of claim 10, wherein the request to access the local memory comprises a request to read data from the local memory.

('571, 30:32-34 (Claim 12).)

53. Claim 13 recites:

13. The device of claim 10, wherein the processor is further configured to restrict modification of the owner control information after the owner control information has been stored on the electronic device.

('571, 30:35-38 (Claim 13).)

54. Claim 14 recites:

14. The device of claim 10, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and wherein the owner control information is provided by an external source through a wireless communication channel.

('571, 30:39-43 (Claim 14).)

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

55. Claim 15 recites:

15. The device of claim 14, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

(’571, 30:44-48 (Claim 15).)

56. Claim 16 recites:

16. The device of claim 10, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

(’571, 30:49-51 (Claim 16).)

57. Independent claim 17 recites:

17. A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:

[a] receiving owner information from an owner of an electronic device;

[b] receiving owner control information that comprises:

[b][i] a list of applications permitted for installation on the device, and

[b][ii] permissions associated with each permitted application in the list of applications;

- [c] storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;
- [d] receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;
- [e] determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and
- [f] controlling application access to the local memory based upon the determining.

('571, 30:52-31:9 (Claim 17; bracketed notation (*e.g.*, [a]) added).)

58. Claim 18 recites:

- 18. The non-transitory computer-readable medium of claim 17, wherein the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device.

('571, 31:10-13 (Claim 18).)

59. Claim 19 recites:

- 19. The non-transitory computer-readable medium of claim 17, wherein the request to access the local memory comprises a request to erase data from the local memory.

(’571, 31:14-16 (Claim 19).)

60. Claim 20 recites:

20. The non-transitory computer-readable medium of claim 17,  
wherein the request to access the local memory comprises a  
request to read data from the local memory.

(’571, 31:17-19 (Claim 20).)

## V. APPLICATION OF THE PRIOR ART TO THE CHALLENGED CLAIMS

61. I have reviewed and analyzed the prior art references and materials listed above. In my opinion, the challenged claims of the ’571 patent would have been obvious to a person of ordinary skill in the art based on the following prior art combinations.

| Ground | Claims     | Basis for Challenge Under § 103                        |
|--------|------------|--------------------------------------------------------|
| 1      | 1-20       | Lambert                                                |
| 2      | 1-20       | Ground 1 + Frank, Gomberg, and Windows Guidelines Book |
| 3      | 1-8, 10-20 | Hayes in view of Sprigg                                |
| 4      | 1-8, 10-20 | Ground 3 + Frank and Guedalia                          |
| 5      | 9-20       | Ground 4 + Lambert                                     |

### A. Summary and Overview of Lambert Grounds Prior Art (Grounds 1-2)

#### 1. Lambert (EX1004)

62. **Lambert**, U.S. Patent Application Publication No. 2002/0099952

(filed June 8, 2001, published July 25, 2002), is titled “Policies for Secure Software Execution.” I am informed that Lambert qualifies as prior art because it was both filed and published before the alleged priority date of the ’571 patent.

63. Lambert is directed to a “security framework for computer systems.” (Lambert, [0002].) Like the ’571 patent, Lambert discusses “in enterprise computing environments, system administrators and helpdesk personnel are trained in supporting a core set of programs used in operating the business.” (*Id.*, [0003].) Lambert explains that a known “method to reduce the possible damage that can be done when running unknown applications is for a user to log onto a computer with a user account that has less access rights and/or less privileges than the user would have to system or network resources if logged on with a different user account. This takes advantage of existing computer security system models that determine each user’s access to network resources based on permissions granted according to that user’s credentials, whereby any potential damage done by unknown executable code is limited or contained by the reduced access rights and/or privileges.” (*Id.*, [0006].) But to further improve security, Lambert teaches “various ways to identify/classify software, along with a highly flexible policy-based infrastructure to enforce decisions about whether software can run, and if so, how much the software will be restricted when it runs.” (*Id.*, [0009].)

64. Lambert discloses a security system that can use access tokens that can be associated with a process or applications and that can indicate access restrictions. Lambert discloses that when a process **300** associated with an access token “desires access to an object **302**, the process **300** specifies the type of access it desires (e.g., obtain read/write access to a file object), and the operating system (e.g., kernel) level provides its associated token to an object manager **304**[.]” (Lambert, [0042].) Lambert discloses that “[t]he security mechanism **308** compares the security IDs in the restricted token **210** along with the type of action or actions requested by the process **300**” against an access control list. (*Id.*, [0043].) Then, on the basis of the comparison, the requested access is either allowed or denied. (*Id.*)

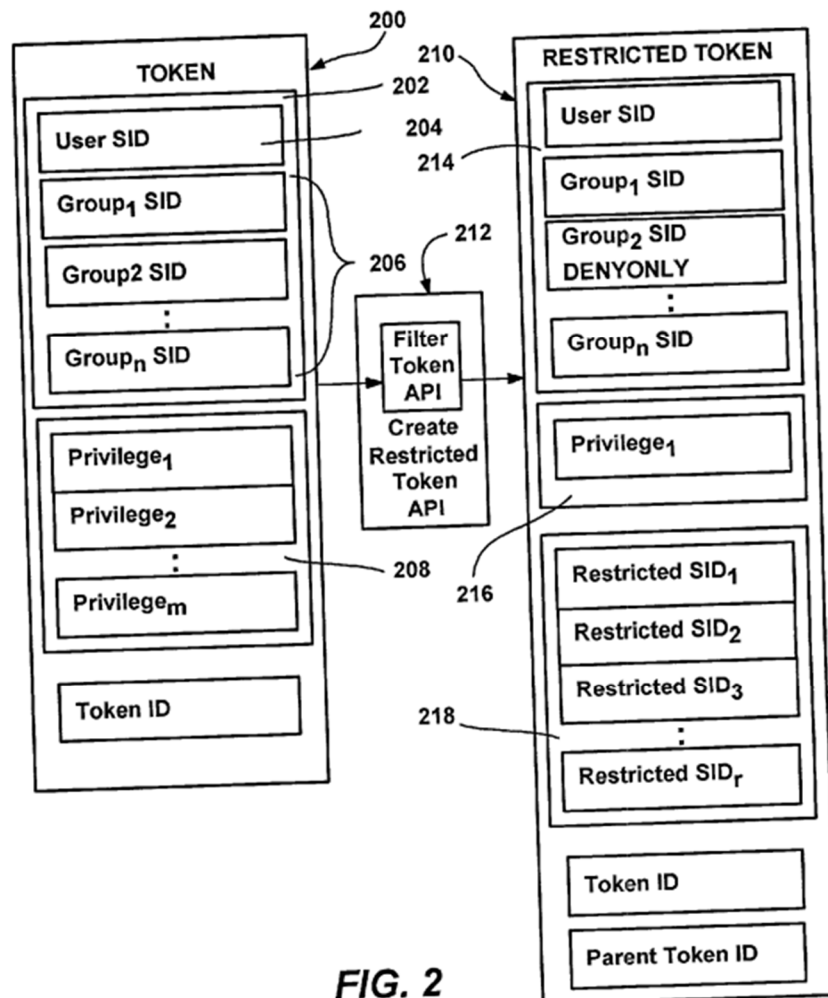


**FIG. 2**

(*Id.*, Fig. 2.)

65. Further, Lambert discloses “a method and system that determines access to resources based on an identification (classification) of software that may contain executable content[.]” (Lambert, [0052].) Lambert discloses that an administrator sets rules for restricting execution of applications based on such identification—including based on “a unique hash value of the file’s content, ... the software’s file system or network path, and/or its origin or source, e.g., its URL

(Uniform Resource Locator) zone.” (*Id.*, [0053]; *see also id.*, [0054]-[0060].) Such rules are “maintained in a restriction policy” for a given user and machine, “e.g., within one or more group policy objects distributable over a network.” (*Id.*, [0064].) Lambert discloses that “[r]ules can also be set for a user or machine locally and maintained in the local system registry, e.g., under HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER.” (*Id.*)

66. The administrator policy rules are used to manage applications in, for example, the system shown in Figure 5A of Lambert:

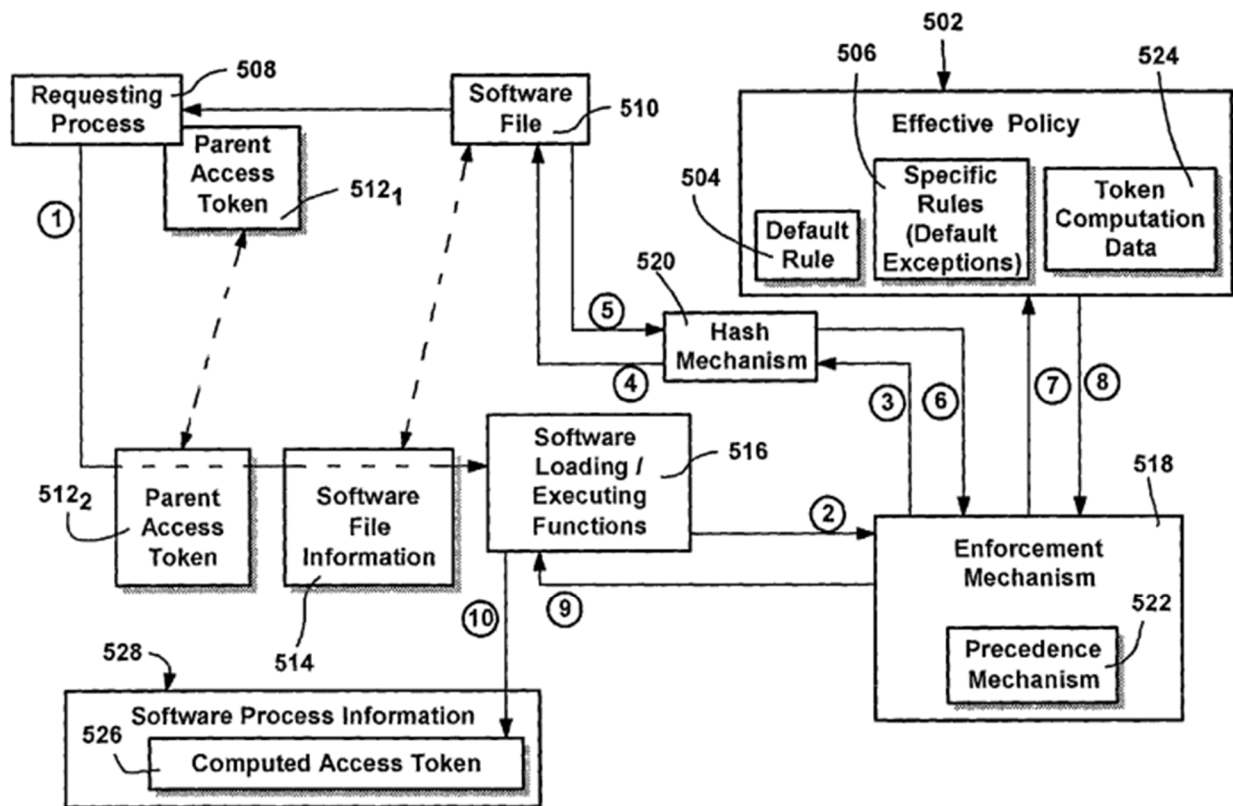


**FIG. 5A**

(Lambert, Fig. 5A, [0065].) Lambert discloses that “a process **508** such as a process of a user or application requesting to open a software file **510** has an access token **512** associated with it, (actually maintained by the operating system in protected kernel mode memory when the process is created).” (*Id.*, [0066].) Lambert discloses that “instead of simply loading the file and executing any executable code therein with the parent token's rights and privileges, each of the functions **516** is arranged to first provide the software file information **514** to an enforcement mechanism (circled numeral two (2) in FIG. 5A).” (*Id.*, [0067].) Further, “the enforcement mechanism consults the effective policy **502** to determine which rule applies for the file **510**, and from the rule determines whether to open/execute the file, and if so, the extent of any restricted execution context for the file **510**.” (*Id.*) Lambert discloses that “[t]he various functions **516** that can be arranged to consult the enforcement mechanism **518** include a create process function, a load library (e.g., a dynamic link library) function, a shell execute function, an object creation function (e.g., CoCreateInstance), script running functions and software installer functions.” (*Id.*, [0072].)

67. Lambert provides an example of an administrator policy in paragraph [0082], part of which is reproduced below:

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

|                                                  |                                         |                                          |                                   |
|--------------------------------------------------|-----------------------------------------|------------------------------------------|-----------------------------------|
| OnlySignedLockDown<br>Path                       | HKCU<br>%windir%                        | Disallowed<br>Unrestricted               | CP only<br>All file<br>types      |
| Certificate<br>IexploreOn-<br>lyLockDown<br>Path | <publisher cert><br>HKCU<br>%windir%    | Unrestricted<br>Disallowed               | CP only                           |
| Path                                             | %programfiles%\Internet<br>Explorer\    | Unrestricted                             | All file<br>types                 |
| WMPOnlyLockDown<br>Path                          | HKCU<br>%windir%                        | Disallowed<br>Unrestricted               | CP<br>Only<br>All file<br>types   |
| Path                                             | %programfiles%\<br>Windows Media Player | Unrestricted                             | All file<br>types                 |
| PFNoMediaLockDown<br>Path                        | HKCU<br>%windir%                        | Disallowed<br>Unrestricted               | CP<br>Only<br>All file<br>types   |
| Path                                             | %programfiles%\                         | Unrestricted                             | All file<br>types                 |
| Path                                             | %programfiles%\<br>Windows Media Player | Disallowed                               | All file<br>types                 |
| Hash<br>OfficeAllowLock-<br>AllDown<br>Path      | wmplayer.exe<br>HKCU<br>%windir%        | Disallowed<br>Disallowed<br>Unrestricted | N/A<br>CP/LL<br>All file<br>types |

(Lambert, [0082].)

68. Lambert further discloses setting multiple access policies, which can be applied in access restriction rules. For example, “there may be one authorization level for unrestricted operation, one for end-user, one for constrained, one for untrusted and one for revoked, although more or less than these can be present.”

(Lambert, [0079].)

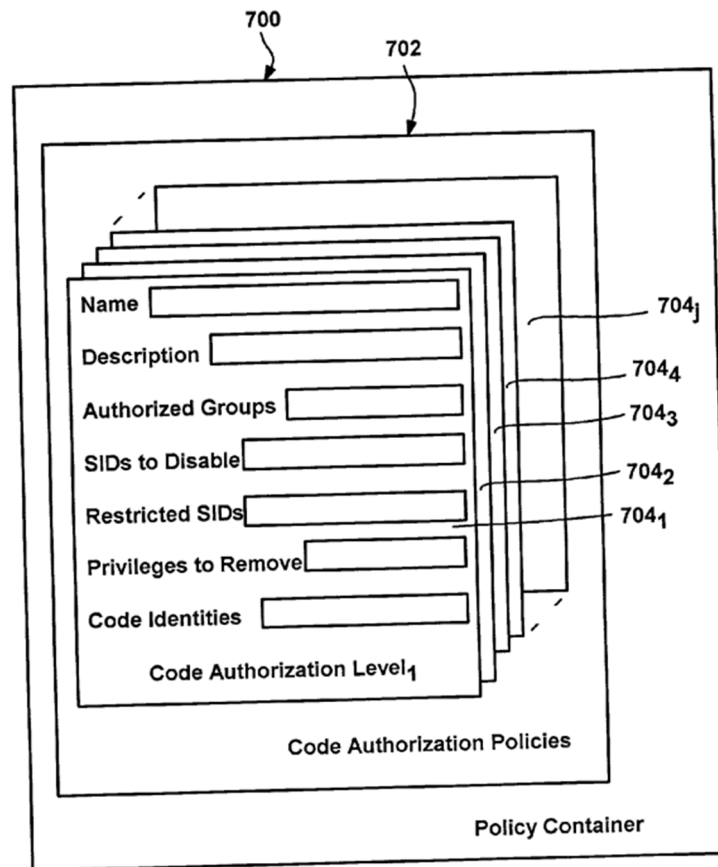
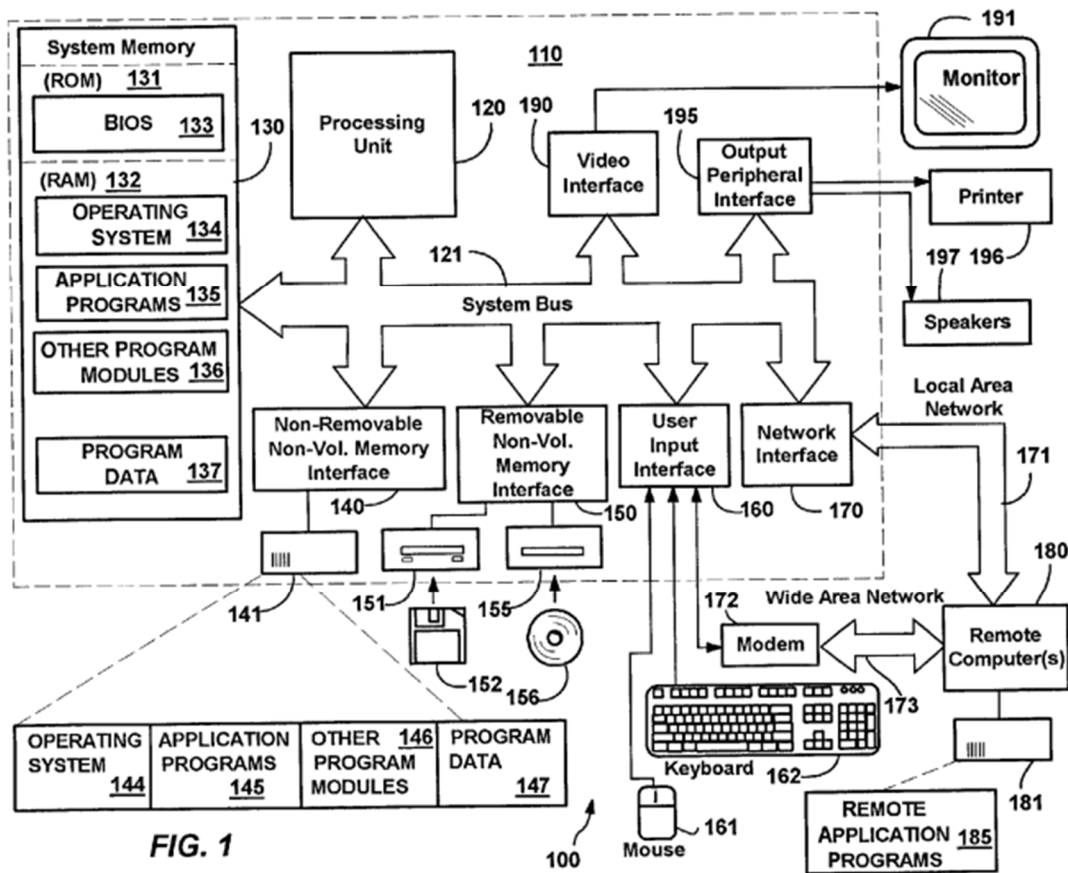


**FIG. 7**

(*Id.*, Fig. 7.)

69. Lambert discloses a computer that can be used in its computer system, as shown in Figure 1:



(Lambert, Fig. 1.) Lambert discloses that “[c]omponents of the computer 110 may include, but are not limited to, a processing unit 120, a system memory 130, and a system bus 121 that couples various system components including the system memory to the processing unit 120.” (*Id.*, [0029].) Further, Lambert discloses that “[t]he system memory 130 includes computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 131 and random access memory (RAM) 132 ,” where “[a] basic input/output system 133 (BIOS), containing the basic routines that help to transfer information between elements

within computer **110**, such as during start-up, is typically stored in ROM **131**” and “RAM **132** typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit **120**.” (*Id.*, [0031].)

## 2. Frank (EX1005)

70. **Frank**, U.S. Patent Application No. 2002/0095572 (filed January 12, 2001, published July 18, 2002) is titled “System and Method for Providing Security Profile Information to a User of a Computer System.” I am informed that Frank qualifies as prior art because it was both filed and published before the alleged priority date of the ’571 patent.

71. Frank discloses an administered computer network where user terminals have a “security application” that allows an administrator to log in to the user terminal, change security settings, and apply those security settings in real time. Frank discloses that its system is responsive to concerns of prior computer network security administration systems, where “the process of selecting which rules should be included in the computer system’s security profile can be a tedious and time consuming process[.]” (Frank, [0010].) Further, Frank discusses that in security administration, “the administrator may make mistakes,” and “the system administrator, due to human error or due to the administrator’s lack of understanding

the ramifications of the changes, may mistakenly add undesirable rules and/or remove desirable rules, thereby changing the security profile in an undesirable way.”

(*Id.*, [0011]; *see also id.*, [0012] (“in some situations, it is possible that the errors introduced by changing the security profile lock authorized users and even the system administrator out of the computer system and/or the security application, thereby making the process of correcting for the administrator's mistakes even more difficult and problematic”).) Frank discloses that debugging security policies in prior systems can be difficult, and “understanding the ramifications of whether or not particular rules are selected is paramount in such a debugging process, and not all system administrators are familiar enough with the security application in order to make well informed decisions in debugging and/or changing the security profile.” (*Id.*, [0012].)

72. Frank discloses that the “security application **13**” on a user terminal “includes data that defines a list of security rules for preventing unauthorized access and/or modification of certain applications **14**, files **15**, and/or other resources within the computer system **12**.” (Frank, [0028].) A system administrator uses the security application to change the securities rules. (*Id.*, [0029].) Then, the administrator can input a request “for activating the selected profile or, in other words, for enforcing the rules selected by the user.” (*Id.*, [0030].) “In other words,

the security profile selected by the system administrator is activated.” (*Id.*)

### 3. Gomberg (EX1006)

73. **Gomberg**, titled “A Comparison of Large-Scale Software Installation Methods on NT and UNIX,” was published in the “Proceedings of the Large Installation System Administration of Windows NT Conference Seattle, Washington, August 5-8, 1998.” (EX1006.) I am informed that Gomberg qualifies as prior art because it was published at least as early as September 1998.

74. As Gomberg recognizes, the “Mathematics and Computer Science Division of Argonne National Laboratory consists of nearly a thousand computers, including supercomputers, servers, workstations, desktop machines, and laptops. The majority of these are running UNIX, but the number of NT machines is steadily growing, particularly on desktops.” (Gomberg, p.002.)<sup>3</sup> By 1998, UNIX and NT

---

<sup>3</sup> Argonne National Laboratory is a research and development (“R&D”) center in Lemont, Illinois. (EX1008, <https://www.anl.gov/argonne-national-laboratory>.) Argonne is owned by the United States Department of Energy. (See EX1009, <https://www.energy.gov/ea/argonne-national-laboratory>.) Argonne was “born out of the University of Chicago’s work on the Manhattan Project in the 1940s,” with

machines were both widely available.

75. Gomberg discloses that in its administered computer network, there is a feature called “package command manager.” (Gomberg, p.007.) This feature “allows the administrator to specify software ‘packages’ that can be installed on workstations in one of two ways.” (*Id.*) First, Gomberg discloses that the administrator “can schedule compulsory software packages that will be installed at a certain time.” (*Id.*) Second, Gomberg discloses that “[f]or optional software, the user can be presented with a list of software that can be installed at login.” (*Id.*) Gomberg discloses that the second option is advantageous, because it “helps with the problem of buying licenses that you don’t need, allocating expensive software packages only to those who need them.” (*Id.*)

#### 4. **Windows Guidelines Book (EX1010)**

76. The **Windows Guidelines Book**, titled *The Windows Interface Guidelines for Software Design* (“Windows Guidelines Book”), is a book published in 1995 by the Microsoft Corporation. (EX1010.) I am informed that the Windows Guidelines Book qualifies as prior art because it was published at least as early as

---

the goal “to make an impact — from the atomic to the human to the global scale.” (EX1008, <https://www.anl.gov/argonne-national-laboratory>.)

December 1995.

77. The Windows Guidelines Book indicates that it is an “indispensable guide to designing software that runs with the Microsoft® Windows® operating system” and is “intended for those who are designing and developing Windows-based software” and “may also be appropriate for those interested in a better understanding of the Windows environment and the human-computer interface principles it supports.” (Windows Guidelines Book, pp.003-004.) It further indicates that “[t]his guide promotes good interface design and visual and functional consistency within and across Windows-based applications.” (*Id.*, p.003.) The Windows Guidelines Book indicates that it covers, for example, “[b]asic design principles and process”; “[i]nterface elements,” *i.e.*, “descriptive information about the various components in the interface as well as when and how to use them”; “[d]esign details,” *i.e.*, “specific information about the details of effective design and style when using the elements of the interface”; and “summary and quick reference information[.]” (*Id.*, p.004.)

78. The Windows Guideline Book describes “Adding to the Passwords Object.” (Windows Guidelines Book, pp.006-007.) The Windows Guidelines Book indicates that “[t]he Passwords object in Control Panel supplies a property sheet that allows the user to set security options and manage passwords for all password-

protected services in the system." (*Id.*, p.006.) Further, "[t]he Passwords object ... allows you to add the name of a password-protected service to the object's list of services and use the Windows login password for all password-protected services in the system." (*Id.*) A user can also either "choose[] to keep the password for the service identical to the Windows login password" or "the user can disassociate the service from the Windows login password by toggling [a] check box setting off." (*Id.*, p.007.)

79. The Windows Guidelines Book discloses that "[w]hen you add your service to the Passwords object, the name of the service appears in the Select Password dialog box that appears when the user chooses Change Other Passwords." (Windows Guidelines Book, p.007.) "The user can then change the password for the service by selecting the name and filling in the resulting dialog box." (*Id.*)

80. The Windows Guidelines Book indicates that "[t]o add your service to the Passwords object, register your service under the **HKEY\_LOCAL\_MACHINE** key." (Windows Guidelines Book, p.007.) The Windows Guidelines Book provides the following diagram:

**HKEY\_LOCAL\_MACHINE**

**System**

**CurrentControlSet**

**Control**

**PwdProvider**

***Provider Name Value Name = Value***

(*Id.*)

81. The Windows Guidelines Book further discloses that “[y]ou can ... add a page to the property sheet of the Passwords object to support other security-related services that the user can set as property values.” (Windows Guidelines Book, p.007.) The Windows Guidelines Book indicates that a user can “[a]dd a property page if [an] application provides security-related functionality beyond simple activation and changing of passwords.” (*Id.*)

**B. Grounds 1-2: Claims 1-20 are Obvious Over Lambert  
(Ground 1); Claims 1-20 are Obvious Over Lambert in View of  
Frank, Gomberg, and Windows Guidelines Book (Ground 2)**

| <b>Ground</b> | <b>Claims</b> | <b>Basis for Challenge Under § 103</b>                 |
|---------------|---------------|--------------------------------------------------------|
| 1             | 1-20          | Lambert                                                |
| 2             | 1-20          | Ground 1 + Frank, Gomberg, and Windows Guidelines Book |

**1. Independent Claim 1**

**(a) “A method of application control on an electronic device, the method comprising:”  
(Claim 1[p])**

82. It is my opinion that claim 1[p] is disclosed by Lambert.

83. As Lambert recognizes, “**electronic device[s]**” were well-known. Lambert’s techniques are “operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.” (Lambert, [0027] (emphasis added).)

84. Lambert discloses controlling execution of applications on an electronic device (“[a] **method of application control on an electronic device**”) depending on rules, including based on user access tokens, for what resources particular applications or application types are allowed to access. For example, Lambert discloses that “the present invention automatically controls whether content is executable, and if so, the extent (if any) to which it is restricted.” (Lambert, [0054] (emphasis added); *see also id.*, [0101] (describing invention as “a framework that controls the execution of software in accordance with a restriction policy”), [0050] (“The design of restricted tokens provides for significant flexibility and granularity

within the context of a user to control what different processes are allowed to do.” (emphasis added)), [0052] (“by allowing the administrator to set a default rule, an administrator can efficiently control software in any environment” (emphasis added)), [0022] (describing “controlling software execution in accordance with one aspect of the present invention” (emphasis added)), [0058] (describing “using conventional access control technology, such as via discretionary access control lists”), [0008] (describing invention as “an improved computer security system and method”).)

85. Lambert’s method operates “**on an electronic device**”—*e.g.*, on a computer via control software controlling execution of software on the computer based on information (tokens, rules, etc.) stored on the computer. (*E.g.*, Lambert, [0028] (“The invention may be described in the general context of computer-executable instructions, such as program modules, being executed by a computer.”), [0066] (discussing access token “maintained by the operating system in protected kernel mode memory”), [0031]-[0032], [0038], [0052].)

86. As explained below, Lambert discloses and renders obvious the “**method of application control on an electronic device**” as claimed. (*See also* Lambert, Abstract (“The security level may disallow the software’s execution, restrict the execution to some extent, or allow unrestricted execution. To restrict

software, a restricted access token may be computed that reduces software's access to resources, and/or removes privileges, relative to a user's normal access token.".)

**(b) "receiving, by the electronic device, owner information from an owner of the electronic device;" (Claim 1[a])**

87. It is my opinion that claim 1[a] is disclosed by or would have been obvious based on Lambert.

88. Lambert teaches the claimed **"owner information,"** such as administrator credentials. Lambert's administrator credentials are **"owner information"** because they are identifying credentials of an administrator of a network, including on a corporate network where administrators operate on behalf of the **"owner"**—*e.g.*, a company. (Lambert, [0012] ("In an enterprise environment, the policy may be set for sites, domains, organizational units, groups and/or users via group policy technology."), [0003] ("in enterprise computing environments, system administrators and helpdesk personnel are trained in supporting a core set of programs used in operating the business.")) Lambert's "owner information" is **"from an owner of the electronic device."** (*E.g., id.*, [0008]-[0009], [0003]-[0006], [0011]-[0012].)

89. Much like Lambert, the '571 patent is aimed at owner information provided by network administrators. (*E.g.*, '571 patent, 5:63-67 ("Where the electronic device **210** is provided to a user by an employer, for example, the

owner control insertion point **220** may be a computer system or device controlled by a corporate computer system administrator or IT department.”) (emphasis added), 6:44-50 (“In a large company, for example, corporate computer system administrators may be authorized to perform owner information insertion operations from administrator computer systems, or from any corporate computer system from which administrative functions can be accessed, thereby providing multiple owner information insertion points **220.**”) (emphasis added), 11:37-40 (“at least a first owner information insertion operation for any mobile device **30** is preferably either performed or at least authorized by an administrator”) (emphasis added), 19:14-17 (“initial owner information insertion may be performed directly by or at least under the authorization of the owner or an owner system administrator”) (emphasis added), 9:11-17 (discussing an “owner system administrator”), 8:7-10, 10:58-62.)

90. Lambert discloses that information (*e.g.*, credentials) are “**receiv[ed], by the electronic device.**” Specifically, Lambert teaches “**receiving, by the electronic device, owner information from an owner of the electronic device.**” For example, Lambert discloses that the user interface for making policy changes can be accessible on any computer in the network “at least by an administrator.” (Lambert, [0081]; *see also id.*, [0100].) Lambert further discloses that administrator policy rules can be “set for a user or machine locally and maintained in the

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

local system registry, e.g., under HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER.” (*Id.*, [0064]; *see also id.*, [0078] (“the administrator (or the user) may construct and locally maintain local machine policy **610** and local user policy **612**, such as in the system registry”), Abstract, [0028] (“The invention may be described in the general context of computer-executable instructions, such as program modules, being executed by a computer.”) (emphasis added).) Lambert further teaches that administrative credentials enable a user to make various changes to administrator policy settings that cannot be made using non-administrative (or less highly privileged administrative) credentials. (*Id.*, Abstract; *see also id.*, [0057] (“the user interface provides an option that determines exactly who can specify which publishers are trusted, e.g., a domain administrator, any administrator, and/or an end user, with any higher-level administrator able to block those below from changed the setting”), [0100] (“Note that instead of restricting (or completely denying) access, a dialog box or the like may be provided to allow a user to override the decision, possibly requiring more powerful (e.g., administrator-level) credentials.”), [0080], [0099]; *see also id.*, [0006] (disclosing “determin[ing] each user’s access to network resources based on permissions granted according to that user’s credentials”), [0038] (describing “[w]hen a user logs on to a secure machine or network (such as one running the Windows® 2000 operating system) and is

authenticated”).) Lambert’s owner information is thus being “**receiv[ed], by the electronic device ... from an owner of the electronic device,**” since administrator credentials would need to be received to ensure that only administrators can make particular policy changes. (*Id.*, [0058] (discussing “conventional access control technology...to prevent the user from writing to the system directory”), [0006].) Lambert teaches that an administrator could provide the policy rules on the computer where those rules are then enforced (*e.g.*, for other non-administrative users). (*Id.*, [0078] (“the administrator (or the user) may construct and locally maintain local machine policy **610** and local user policy **612**, such as in the system registry”), [0064].) Lambert thus teaches or renders obvious “**receiving, by the electronic device, owner information from an owner of the electronic device.**”

### **Obviousness Over Lambert in View of Frank**

91. As I explained above, Lambert discloses or renders obvious claim 1[a]. Claim 1[a] also would have been obvious over Lambert in light of **Frank** (EX1005; U.S. Patent Application No. 2002/0095572).

92. Much like Lambert, Frank discloses a computer security system managed by administrators to control the activity of end users. (Frank, [0002] (“The present invention generally relates to computer resource security[.]”), [0029] (user of security application is “a system administrator (i.e., a user authorized to set and/or

change the security profile of the system **12**)”), [0005]-[0012] (discussing system administrators as “Related Art”).) Frank discloses a security application that an administrator can access on the device for which the administrator is setting security policy—applying the security rules input by the administrator in real time. (*Id.*, [0043] (“In response, the security application **52** modifies the machine state of the computer system **50** such that the security rules selected by the system administrator are enforced by the computer system **50** (e.g., by operating system **16**) during any subsequent operation until the security profile is later changed.”); *id.*, [0040]-[0042], [0028]-[0030] (“In other words, the security application **13** includes data that defines a list of security rules for locking down the computer system **12**.”).) This allows the administrator to see the impact of changing a security policy on the target device immediately, allowing the user to easily see the consequences of the policy in case there are undesirable results and modify the policy accordingly. (*Id.*, [0011] (administrator “may mistakenly add undesirable rules and/or remove desirable rules”), [0012] (in the prior art, “[a]ttempting to discover and remedy the undesirable effects introduced by the system administrator in changing the security profile can be difficult and/or time consuming”).)

93. It would have been obvious to a POSITA to implement Lambert’s system to allow an administrator to set up or adjust the access restriction policy for

a user's computer terminal (either locally or on the server) by using the computer terminal itself. In the combination, an administrator could log in to a user's terminal by providing "**owner information**"—*i.e.*, administrator credentials—to the terminal itself and pull up a security application that would allow the administrator to adjust access restriction policy (whether stored on a server or in local device memory) for the device. Accordingly, in the combination, the user terminal would "**receiv[e], by the electronic device** [*i.e.*, the user terminal], **owner information** [*i.e.*, administrator credentials] **from an owner of the electronic device** [*i.e.*, the administrator using the terminal]."

94. **Motivation to Combine**: Lambert and Frank are analogous art in a similar field. For example, both references relate to administrators setting computer security policy for end users. (Frank, [0002] ("The present invention generally relates to computer resource security[.]"), [0029] (user of security application is "a system administrator (*i.e.*, a user authorized to set and/or change the security profile of the system **12**)"), [0008] ("Normally, a security application only allows the system administrator or a user designated by the system administrator to change the computer system's security profile."), [0005]-[0007], [0009]-[0012]; Lambert, [0078] ("an administrator (possibly multiple administrators) constructs the various polices [sic] that make up the effective policy **502**"), [0002] ("The present invention

is generally directed to computer systems, and more particularly to an improved security framework for computer systems.”), [0080]-[0081], [0003].)

95. A POSITA would have been motivated to implement a security application on a user terminal on Lambert’s system to enable an administrator to easily see the results of changes to security policy. A POSITA would have understood this as advantageous, since it would make it less likely for an administrator to make a change to security policy that causes undesirable results on a user terminal. For example, Lambert discloses that a security policy might create “an error wherein the default rule is set to prevent (revoke) all software from running, which could then otherwise prevent the user interface program **600** from subsequently running to except itself from the default rule.” (Lambert, [0081].) Frank discloses that its system helps avoid just such an error—*i.e.*, “it is possible that the errors introduced by changing the security profile lock authorized users and even the system administrator out of the computer system and/or the security application, thereby making the process of correcting for the administrator’s mistakes even more difficult and problematic.” (Frank, [0012]; *see also id.*, [0011] (discussing “human error” and “administrator’s lack of understanding the ramifications of the changes” to a security policy).) Frank indicates that by allowing an administrator to view the “ramifications” of the selected security policies, its

system allows the administrator to “make better decisions when defining a security profile.” (*Id.*, [0036].) Accordingly, a POSITA would have been motivated to implement a security application like Frank’s on a user terminal to make access restriction policy errors like Lambert discloses less likely. (Lambert, [0081]; *see also id.*, [0058] (discussing security policies to ensure that “the computer will work normally”).)

96. A POSITA would have further been motivated to combine Lambert and Frank to streamline the process of inputting security policy for a computer. A POSITA would have understood that if an administrator could easily see the results of a security policy in real time on a user terminal, this would make it less likely that the security policy would need to go through multiple (potentially time-consuming, costly) iterations. Instead, an administrator could simply adjust the security policy, see the results, and adjust the policy further if necessary—cutting out potentially costly time for a policy to be rolled out to an entire organization and cause issues before being revised. Lambert contemplates the use of its system for the computer network of a business enterprise and indicates that “maintenance and helpdesk time” and “decreased user productivity” are costs to be avoided. (Lambert, [0007].) A POSITA would have understood that streamlining the security policy input process would have decreased the time and costs associated with an administrator’s inputting

of security policy.

97. A POSITA would have been further motivated to implement an administrator security application on a user terminal in Lambert's system because of the fact that formulating security policy for a computer network requires a balancing approach that is fundamentally iterative. For example, Frank discloses that "the degree to which the computer system is locked down by the security application depends on the competing interests of system security and system compatibility." (Frank, [0008].) A POSITA would have understood that navigating such competing interests of setting a security policy would be best suited by seeing the results of such a policy in real time, as Frank's system (and the combination between Lambert and Frank) allows.

98. A POSITA would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques without undue experimentation. The Lambert and Frank combination is standard computing technology. The proposed combination would have involved nothing more than the routine implementation of known techniques.

99. Lambert and Frank are both analogous references to the '571 patent. Both Lambert and Frank relate to establishing and determining computer security policy for end users by system administrators. (Frank, [0002], [0029], [0036]

(“Thus, the system administrator should better understand the ramifications of selecting the rule for enforcement, and as a result, the system administrator should make better decisions when defining a security profile.”); Lambert, [0078], [0002], [0007]; ’571, 1:41-43, 6:44-50, 1:52-55, 1:63-2:5.)

**Obviousness Over Lambert in View of Windows Guidelines Book**

100. As discussed below for claim 1[c], it would have been obvious to combine Lambert with the Windows Guidelines Book to implement Lambert’s system such that Lambert’s rule-based policy information would be stored in a password-protected registry like HKEY\_LOCAL\_MACHINE in the Microsoft Windows operating system. Thus, claim 1[a] would have further been obvious over Lambert in view of the Windows Guidelines Book, since it would require receiving administrator credentials to store or alter rule-based policy information—*i.e.*, **“receiving, by the electronic device, owner information from an owner of the electronic device.”**

**(c) “receiving, by the electronic device, owner control information that comprises:” (Claim 1[b])**

101. It is my opinion that claim 1[b] is disclosed by and/or would have been obvious based on Lambert.

102. Lambert teaches **“receiving, by the electronic device, owner control information.”** As discussed above, Lambert discloses that an administrator

provides a network computer with “**owner control information.**” Lambert discloses that an administrator provides a policy in the form of rules for what processes are allowed to execute on a computer. (Lambert, [0061]-[0065], [0080]; *see also id.*, [0008] (“A set of rules for a machine or user may be maintained in a restriction policy, e.g., in a group policy object distributable over a network, and a restriction policy can be applied per machine and/or per user of a machine.”), [0011], [0052] (“An administrator identifies/classifies the software and sets the rules[.]”), [0056], [0078] (“the administrator (or the user) may construct and locally maintain local machine policy **610** and local user policy **612**, such as in the system registry”).) The rules are used by an enforcement mechanism **518**, which monitors processes on the computer and provides an instruction on whether a given process can execute, or whether it can execute under certain restrictions. (*E.g., id.*, [0068]-[0071].)

103. Lambert’s rule-based policy information constitutes “**owner control information.**” They are rules provided by an administrator of a network, including on a corporate network where administrators operate on behalf of the owner—*i.e.*, a company. (Lambert, [0012] (“In an enterprise environment, the policy may be set for sites, domains, organizational units, groups and/or users via group policy technology.”), [0003] (“in enterprise computing environments, system

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

administrators and helpdesk personnel are trained in supporting a core set of programs used in operating the business”).) Such an understanding is consistent with the ’571 patent, which describes owner control information provided by network administrators. (’571 patent, 5:63-67 (“Where the electronic device **210** is provided to a user by an employer, for example, the owner control insertion point **220** may be a computer system or device controlled by a corporate computer system administrator or IT department.” (emphasis added)), 6:44-50 (“In a large company, for example, corporate computer system administrators may be authorized to perform owner information insertion operations from administrator computer systems, or from any corporate computer system from which administrative functions can be accessed, thereby providing multiple owner information insertion points **220**.”), 11:37-40 (“at least a first owner information insertion operation for any mobile device **30** is preferably either performed or at least authorized by an administrator” (emphasis added)), 19:14-17 (“initial owner information insertion may be performed directly by or at least under the authorization of the owner or an owner system administrator”), 9:11-17 (discussing an “owner system administrator”), 8:7-10, 10:58-62.)

104. Furthermore, Lambert discloses that administrator policy rules are “receiv[ed] by the electronic device.” Lambert discloses that administrator policy

rules can be “set for a user or machine locally and maintained in the local system registry, e.g., under HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER.” (Lambert, [0064]; *see also id.*, [0078] (“the administrator (or the user) may construct and locally maintain local machine policy **610** and local user policy **612**, such as in the system registry”), [0079], [0081], Abstract, [0028].) Thus, Lambert discloses that an administrator could provide the policy rules on the computer where those rules are then enforced (*e.g.*, for other non-administrative users).

105. Lambert also discloses that administrator policy rules can be input by an administrator over a computer network. (Lambert, [0064] (“The set of rules for a machine or user may be maintained in a restriction policy for that user and machine, e.g., within one or more group policy objects distributable over a network, to correlate the classification information for any software file to a security level that may restrict or prevent the software from running.”); *see also id.*, Abstract, [0008] (“group policy distributed over a network”), [0028].) Lambert discloses that an administrator can input policy rules from any computer on a network. For example, Lambert discloses that “one policy that may be desirable for all users and machines and should not be overridden is one that allows the user interface program **600** to be run (at least by an administrator) regardless of the default rule[.]” (*Id.*, [0081] (emphasis added); *see also id.*, [0099], [0101], [0010], [0057].) This indicates that

any computer on a network could receive administrator policy rules input by the administrator—*i.e.*, “**receiving, by the electronic device, owner control information.**” Additionally, Lambert discloses that network computers can receive administrator policy rules from a server—another form of “**receiving, by the electronic device, owner control information.**” (*Id.*, [0064] (“The set of rules for a machine or user may be maintained in a restriction policy for that user and machine, e.g., within one or more group policy objects distributable over a network, to correlate the classification information for any software file to a security level that may restrict or prevent the software from running.”); *see also id.*, Abstract, [0008] (“group policy distributed over a network”), [0028].)

106. Additionally, as discussed above, it would have been obvious over Lambert in view of Frank to allow an administrator to provide restriction policy rules via the same computer on which those rules are enforced.

**(d) “a list of applications permitted for installation on the electronic device, and” (Claim 1[b][i])**

107. It is my opinion that claim 1[b][i] is disclosed by and/or would have been obvious based on Lambert. In the alternative, it is my opinion that claim 1[b][i] would also have been obvious over Lambert in view of **Gomberg** (EX1006; Michail Gomberg et al, “A Comparison of Large-Scale Software Installation Methods on NT and UNIX” (1998).)

**Lambert Alone Discloses and Renders Obvious Claim 1[b][i]**

108. Lambert discloses that the administrator policy rules (“**owner control information**”) comprise “**a list of applications permitted for installation on the electronic device.**” Lambert teaches that an administrator provides a policy in the form of rules for what processes are allowed to execute on a computer. (*E.g.*, Lambert, [0064]-[0065], [0080].) The rules are used by an enforcement mechanism **518**, which monitors processes on the computer and provides an instruction on whether a given process can execute or whether it can execute under certain restrictions. (*E.g.*, *id.*, [0068]-[0071].) Lambert discloses that one of the types of processes that can be controlled and limited by the administrator policy and enforcement mechanism **518** is that of “software installer functions.” (*Id.*, [0072] (“the software installer function may call the enforcement mechanism **518** only once for an entire installation rather than separately throughout the installation process”).) The table provided in paragraph [0082] of Lambert shows an example of such a policy, with each row listing a rule:

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

|                    |                         |              |          |                   |                           |              |          |
|--------------------|-------------------------|--------------|----------|-------------------|---------------------------|--------------|----------|
| OnlySignedLockDown | HKCU                    | Disallowed   | CP only  | Path              | %programfiles%\micro-     | Disallowed   | <exact   |
| Path               | %windir%                | Unrestricted | All file |                   | soft\office\office\pow-   |              | match>   |
| Certificate        | <publisher cert>        | Unrestricted | CP only  | Path              | erpoint.exe               | Disallowed   | <exact   |
| IexploreOn-        | HKCU                    | Disallowed   |          |                   | %programfiles%\micro-     |              | match>   |
| lyLockDown         |                         |              |          |                   | soft\office\office\front- |              |          |
| Path               | %windir%                | Unrestricted | All file | Path              | pg.exe                    | Disallowed   | <exact   |
|                    | %programfiles%\Internet | Unrestricted | All file |                   | %programfiles%\micro-     |              | match>   |
|                    | Explorer\               |              | types    |                   | soft\office\office\out-   |              |          |
| WMPOnlyLockDown    | HKCU                    | Disallowed   | CP       | NoAttachments-    | look.exe                  | Unrestricted | CP/LL    |
|                    |                         |              | LockAll  |                   | HKCU                      |              |          |
| Path               | %windir%                | Unrestricted | All file | Path              | %USERPRO-                 | Disallowed   | All file |
|                    | %programfiles%\         | Unrestricted | types    |                   | FILE%\local               |              | types    |
|                    | Windows Media Player    |              | All file |                   | settings\tempomry         |              |          |
| PFNoMediaLockDown  | HKCU                    | Disallowed   | CP       | DangerousAppsLock | internet files\OLK*       |              |          |
|                    |                         |              | Only     |                   | HKCU                      | Unrestricted | CP       |
| Path               | %windir%                | Unrestricted | All file | Hash              | Regedit.exe               | Disallowed   | N/A      |
|                    |                         |              | types    | Hash              | Regedit32.exe             | Disallowed   | N/A      |
| Path               | %programfiles%\         | Unrestricted | All file | Path              | cmd.exe                   | Disallowed   | N/A      |
|                    |                         |              | types    |                   | %WINDIR%\sys-             |              | <exact   |
| Path               | %programfiles%\         | Disallowed   | All file | Path              | tem32\cmd.exe             |              | match>   |
|                    | Windows Media Player    |              | types    |                   | %WINDIR%\sys-             | Disallowed   | <exact   |
|                    | wmplayer.exe            | Disallowed   | N/A      |                   | tem32\regedit.exe         |              | match>   |
| Hash               | HKCU                    | Disallowed   | CP/LL    | Path              | %WINDIR%\sys-             | Disallowed   | <exact   |
| OfficeAllowLock-   |                         |              |          |                   | tem32\regedit32.exe       |              | match>   |
| AllDown            |                         |              |          |                   | HKLM                      | Unrestricted | CP/LL    |
| Path               | %windir%                | Unrestricted | All file | InnocuousLockAll- |                           |              |          |
|                    |                         |              | types    | Machine           |                           |              |          |
| Path               | %programfiles%\micro-   | Unrestricted | All file | Path              | %windir%\sys-             | Unrestricted | <exact   |
|                    | soft\office             |              | types    |                   | tem32\GDI32.DLL           |              | match>   |
| OfficeWordOnly-    | HKCU                    | Disallowed   | CP/LL    | Path              | %windir%\sys-             | Unrestricted | <exact   |
| AllDown            |                         |              |          |                   | tem32\ntdll.dll           |              | match>   |
| Path               | %programfiles%\micro-   | Disallowed   | <exact   | Hash              | %windir%\sys-             | Unrestricted | <exact   |
|                    | soft\office\office\ex-  |              | match>   |                   | tem32\shell32.dll         |              | match>   |
|                    | cel.exe                 |              |          |                   |                           |              |          |

(*Id.*, [0082].) A larger excerpt of [0082] is reproduced here:

|                    |                         |              |          |
|--------------------|-------------------------|--------------|----------|
| OnlySignedLockDown | HKCU                    | Disallowed   | CP only  |
| Path               | %windir%                | Unrestricted | All file |
|                    |                         |              | types    |
| Certificate        | <publisher cert>        | Unrestricted |          |
| IexploreOn-        | HKCU                    | Disallowed   | CP only  |
| lyLockDown         |                         |              |          |
| Path               | %windir%                | Unrestricted | All file |
|                    |                         |              | types    |
| Path               | %programfiles%\Internet | Unrestricted | All file |
|                    | Explorer\               |              | types    |
| WMPOnlyLockDown    | HKCU                    | Disallowed   | CP       |
|                    |                         |              | Only     |
| Path               | %windir%                | Unrestricted | All file |
|                    |                         |              | types    |
| Path               | %programfiles%\         | Unrestricted | All file |
|                    | Windows Media Player    |              | types    |
| PFNoMediaLockDown  | HKCU                    | Disallowed   | CP       |
|                    |                         |              | Only     |

(*Id.* (excerpt).)

109. The administrator policy in Lambert’s system (including the one shown in the table in paragraph [0082]) is “a list of applications permitted for installation

**on the electronic device.”** The policy lists applications that can be installed on the device—including Internet Explorer and Windows Media Player in the example shown above. (Lambert, [0072].) Further, Lambert discloses that the policy can restrict what is **“permitted for installation”**—*e.g.*, “software installer functions.” (*Id.*)

110. I understand that in the parallel district court litigation, Petitioner proposed that the term “a list of applications permitted for installation” should be construed as “a list of applications permitted by the owner for installation.” Patent Owner proposes no construction needed. In my opinion, Lambert discloses claim 1[b][i] under Petitioner’s proposed construction of this term. Lambert discloses that the administrator policy is provided by an administrator, including in a corporate context where such an administrator is acting on behalf of the owner (*e.g.*, the corporation). Accordingly, the list of applications in the software policy are “permitted by the owner,” since they are permitted by the administrator. Lambert’s rules are a list of applications permitted by the owner for installation. Lambert thus satisfies claim 1[b][i] under any reasonable construction.

111. Lambert thus teaches or renders obvious **“receiving, by the electronic device, owner control information that comprises: a list of applications permitted for installation on the electronic device.”**

**Lambert In View of Gomberg Also Renders Claim 1[b][i] Obvious**

112. As explained above, it is my opinion that claim 1[b][i] is disclosed by or obvious in view of Lambert alone. But if further detail is needed for the claimed “**list of applications permitted for installation on the electronic device**,” this limitation would have been obvious over Lambert in light of **Gomberg** (EX1006; Michail Gomberg et al, “A Comparison of Large-Scale Software Installation Methods on NT and UNIX” (1998).)

113. Lambert in view of Gomberg renders the claimed “**list of applications permitted for installation on the electronic device**” obvious, because Gomberg discloses that in an administered computer network, the computers can provide users with options for software to download at login. Gomberg discloses that “[f]or optional software, the user can be presented with a list of software that can be installed at login.” (Gomberg, p.007 (emphasis added).) Gomberg discloses the benefits of such functionality, such as because it “helps with the problem of buying licenses that you don’t need, allocating expensive software packages only to those who need them.” (*Id.*)

114. **Motivation to Combine**: A POSITA would have been motivated to combine Lambert and Gomberg, including based on Gomberg’s disclosures. Gomberg discloses that providing users with a list of applications permitted for

installation and allowing users to choose what applications to install “helps with the problem of buying licenses that you don’t need, allocating expensive software packages only to those who need them.” (Gomberg, p.007.) A POSITA would have understood Gomberg’s software licensing concerns to be relevant in the context of a corporate computer network like Lambert discloses. (Lambert, [0012], [0003].) For example, Lambert discloses that disadvantages of the prior art include “increased support costs in system maintenance and helpdesk time[.]” (*Id.*, [0007].) A POSITA would have considered software licensing costs in an enterprise computer network to be an additional cost that should be minimized, along with the other costs that Lambert discloses.

115. Lambert and Gomberg are analogous art in a similar field. For example, both references relate to administered computer networks. (Lambert, [0078] (“an administrator (possibly multiple administrators) constructs the various polices [sic] that make up the effective policy **502**”), [0002] (“The present invention is generally directed to computer systems, and more particularly to an improved security framework for computer systems.”), [0080]-[0081], [0003]; Gomberg, p.007 (“This allows the administrator to specify software ‘packages’ that can be installed on workstations in one of two ways.”), p.002 (“This set of machines is managed by a group of seven system administrators[.]”) Further, both references

discuss the use of their systems in the context of the Microsoft Windows operating system. (Lambert, [0037], [0038], [0082]; Gomberg, p.002.)

116. A POSITA would have been motivated to combine Lambert and Gomberg to make Lambert's policies more transparent and user friendly. Lambert discloses restricting applications and processes, including "software installer functions." (Lambert, [0072].) A POSITA would have understood that there would be advantages to communicating allowed and restricted applications and processes to a user. For example, a POSITA would have understood that on a computer within an administered network, a user might assume that applications are *not* allowed until told otherwise. As a result, users might not be able to benefit from certain software even though it is allowed on the system, because the user is not aware that the software is allowed. A POSITA would have understood that the obvious solution to this issue would be to provide the user with a list of optional software for download at login like what Gomberg discloses. A POSITA would have understood that providing such a list of applications permitted for installation would confirm for the user that software tools the user recognizes and desires to install are allowed. Furthermore, the list of applications might teach a user about allowed applications the user was not aware of (*e.g.*, applications the user had not previously known about), giving the user the opportunity to incorporate those tools

into their work.

117. Further, a POSITA would have been motivated to look to Gomberg for detail on how to implement Lambert’s restriction of “software installer functions.” Gomberg discusses details for how such restrictions would have been implemented in a system. (Gomberg, p.007.)

118. It would have been obvious in light of Gomberg to implement Lambert to provide users with a list of software for installation at login. In the combined system, when a user logs in to a network workstation, the user would receive “**a list of applications permitted for installation**” on the workstation by the network administrators. For example, a user would be shown a prompt containing applications allowed by the administrator policy—*e.g.*, Internet Explorer and Windows Media Player. Based on the user’s role and how the user intends to use the workstation, the user would select the software that he or she would like to install on the workstation.

119. A POSITA would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques without undue experimentation. The Lambert and Gomberg combination is standard computing technology. The proposed combination would have involved nothing more than the routine implementation of

known techniques.

120. Gomberg, like Lambert, is analogous art to the '571 patent. Gomberg is in the field of administered computer networks and streamlining administration of access and use of applications. (Gomberg, p.007 (“This allows the administrator to specify software ‘packages’ that can be installed on workstations in one of two ways.”), p.002 (“This set of machines is managed by a group of seven system administrators[.]”); '571, 1:52-55, 1:63-2:5.)

121. Lambert in view of Gomberg thus renders obvious receiving administrator policy rules (“**owner control information**”) that comprise “**a list of applications permitted for installation on the electronic device.**”

(e) “**permissions associated with each permitted application in the list of applications;**” (Claim 1[b][ii])

122. It is my opinion that claim 1[b][ii] is disclosed by or would have been obvious based on Lambert. Lambert teaches administrator policy rules (“**owner control information**”) that comprise the claimed “permissions” in several different ways.

**Unrestricted / Disallowed Permissions**

123. Lambert teaches “**permissions associated with each permitted application in the list of applications.**” For example, the table in paragraph [0082] indicates that different applications are “Unrestricted” or “Disallowed”:

|                                                  |                                         |                                            |                                 |
|--------------------------------------------------|-----------------------------------------|--------------------------------------------|---------------------------------|
| OnlySignedLockDown<br>Path                       | HKCU<br>%windir%                        | Disallowed<br>Unrestricted                 | CP only<br>All file<br>types    |
| Certificate<br>IexploreOn-<br>lyLockDown<br>Path | <publisher cert><br>HKCU<br>%windir%    | Unrestricted<br>Disallowed<br>Unrestricted | CP only<br>All file<br>types    |
| Path                                             | %programfiles%\Internet<br>Explorer\    | Unrestricted                               | All file<br>types               |
| WMPOnlyLockDown<br>Path                          | HKCU<br>%windir%                        | Disallowed<br>Unrestricted                 | CP<br>Only<br>All file<br>types |
| Path                                             | %programfiles%\<br>Windows Media Player | Unrestricted                               | All file<br>types               |
| PFNoMediaLockDown                                | HKCU                                    | Disallowed                                 | CP<br>Only                      |

(Lambert, [0082] (excerpt, color added).) These are permissions associated with each application in the list of applications, as described above. Lambert explains: “security levels for execution (arbitrarily named herein) may include normal (unrestricted), constrained (restricted) or disallowed (revoked), although other levels such as end-user and untrusted are possible, and customized levels can be defined.” (*Id.*, [0013].) “[T]he administrator can create a path rule using an environment variable to that specifies that anything in the “%WINDIR% directory or below runs normally, i.e., unrestricted.” (*Id.*, [0061].)

124. Lambert’s administrator policy teaches “**permissions associated with each permitted application in the list of applications.**” Lambert discloses that an

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

administrator provides a policy in the form of rules for what processes are allowed to execute on a computer. (*E.g.*, Lambert, [0064]-[0065], [0080].) The rules are used by an enforcement mechanism **518**, which monitors processes on the computer and provides an instruction on whether a given process can execute or whether it can execute under certain restrictions. (*E.g., id.*, [0068]-[0071].) Lambert teaches an example administrator policy in paragraph [0082], reproduced below:

[illegible]

(*Id.*, [0082].) Lambert teaches “[a] system and method that automatically, transparently and securely controls software execution by identifying and classifying software, and locating a rule and associated security level for executing executable software.” (*Id.*, Abstract (emphasis added).) “The security level may disallow the software’s execution, restrict the execution to some extent, or allow unrestricted execution. To restrict software, a restricted access token may be computed that reduces software’s access to resources, and/or removes privileges, relative to a user’s

normal access token.” (*Id.*; *see also id.*, [0099] (“If neither allowed or disallowed, the security level indicates some level of restriction.”), Abstract, [0008]-[0009], [0011], [0013], [0054], [0056], [0064], [0072].) Lambert further explains that existing techniques also “take[] advantage of existing computer security system models that determine each user’s access to network resources based on permissions granted according to that user’s credentials”. (*Id.*, [0006] (emphasis added).)

### **Tokens Permissions**

125. Lambert’s tokens also constitute “**permissions associated with each permitted application in the list of applications.**” Lambert discloses that the enforcement mechanism **518** can be instructed based on the administrator policy to restrict the activity of applications by providing a “restricted token.” (Lambert, [0070]-[0071].) The enforcement mechanism **518** “associate[s] a restricted token” with a software application. (*Id.*, [0070].) The restricted token then “establishes a restricted execution environment/context for the processes” of the application, “thus providing the rule-determined secure execution environment.” (*Id.*, [0071].) For example, the restricted token can limit the types of processes the application can do, including whether it has “read-write access to a file object.” (*Id.*, [0072], [0042].)

126. Lambert’s tokens are “**permissions associated with each permitted application in the list of applications.**” The tokens—either restricted or

unrestricted “parent tokens”—are “associate[d]” with a computer’s software applications. (Lambert, [0042], [0047], [0048], [0066], [0070], [0071].) The tokens also provide “**permissions**”—*i.e.*, they indicate what processes can and cannot execute. (*Id.*, [0043], [0047], [0071]-[0073].) Furthermore, the tokens are “**owner control information**,” since they result from the administrator policy information provided by the network administrator. (*Id.*, [0070]-[0073], [0013]-[0014], [0037], [0042]-[0043], [0047].)

- (f) “**storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;**” (Claim 1[c])

127. It is my opinion that claim 1[c] is disclosed by or would have been obvious based on Lambert.

128. Lambert discloses “**storing, by the electronic device, the owner control information in a protected data store** [an area of memory only accessible with certain administrative credentials] **to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information** [administrative credentials].”

129. Lambert discloses “**storing, by the electronic device, the owner control information.**” Lambert discloses storing application restriction policy

information on an individual user's computer, either "locally maintained and/or in a group policy object distributable over a network." (Lambert, Abstract, [0056] ("the rule along with the hash value is maintained or distributed to the machine, (e.g., via a policy object")), [0079] ("policy container **700** (e.g., user or machine group policy objects, or local user or machine policies)"), [0064], [0008]; *see also id.*, [0055] (disclosing "rules maintained in a policy object, or otherwise made available to the system").)

130. Lambert further discloses storing the owner control information "**in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information.**" As explained above, Lambert discloses that a user interface for adjusting administrator policy settings can be accessed on any machine *only* with administrator privileges. (Lambert, [0081] ("one policy that may be desirable for all user and machines ... is one that allows the user interface program **600** to be run (at least by an administrator) regardless of the default rule"); *see also id.*, [0078] ("via a user interface program **600**, e.g., a management console snap-in, an administrator (possibly multiple administrators) constructs the various policies [sic] that make up the effective policy **502**"), [0055] ("Via a user interface or the like..., an administrator can select any software file, obtain a hash value from its

contents, and enter and associate a rule (that specifies a security level) with that hash value.”), [0056], [0057] (“the user interface provides an option that determines exactly who can specify which publishers are trusted, e.g., a domain administrator, any administrator, and/or an end user, with any higher-level administrator able to block those below from changed the setting”).) Generally, Lambert indicates that its system is intended to remove application access restrictions from the control of individual users and instead placing such control in the hands of administrators, who are better equipped to determine what applications and processes can be trusted. (*Id.*, [0007] (“it is very difficult for individual users to consistently make effective choices about what software they should run”), [0057].) Thus, Lambert discloses “**storing, by the electronic device, the owner control information in a protected data store** [*i.e.*, one that can only be accessed or altered using administrative credentials] **to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information.**”

131. Lambert also teaches that a user’s privileges determine what policy rules a user can change or override, indicating that once certain policy rules (*e.g.*, administrator-set rules, or group policies) are saved to a user’s computer, they cannot be modified by an end user—*i.e.* they are stored in a “**protected data store**” and are made to “**prevent alteration or deletion of the owner control information**” for

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

certain users. (Lambert, [0080] (“site policies can be set up to prevail over domain policies, which in turn can be set up to prevail over organizational unit policies, which can prevail over group and user policies, which can prevail over local policies”), [0057] (“the user interface provides an option that determines exactly who can specify which publishers are trusted, e.g., a domain administrator, any administrator, and/or an end user, with any higher-level administrator able to block those below from changed the setting”), [0100] (“Note that instead of restricting (or completely denying) access, a dialog box or the like may be provided to allow a user to override the decision, possibly requiring more powerful (e.g., administrator-level) credentials.”), [0099], [0039]; *cf. id.*, [0080] (further discussing policies that can be “overridden by lower level policies,” which are “essentially only suggested policies”).)

132. Lambert’s teachings of a protected data store are consistent with the ’571 patent. For example, the ’571 patent suggests storing data “at a location that is accessible to administrator computer systems[.]” (’571, 10:58-62.) “Any data stores” that “store owner information or owner control information can ... be located in protected memory areas” where only the administrator-accessible “insertion module 44 has write and erase access,” and “[o]ther device systems have read only access to owner information and owner control information.” (*Id.*, 13:46-55; *see*

*also id.*, 13:55-62 (“allow[ing] memory read operations from any locations in the memory **32**, but deny[ing] any write or erase operations to memory locations storing owner information or owner control information unless the operations originate with or are authorized by the insertion module **44**”), 9:34-36 (“processor **40** may be configured to start the insertion module **44** whenever owner information is received”).)

133. Lambert also teaches preventing access, and thus “**prevent[ing] alteration or deletion,**” to policy settings stored locally. In particular, Lambert teaches that policy information (“**owner control information**”) can be stored locally in the user’s computing device in the device’s “registry.” (Lambert, *e.g.*, claim 37 (“The method of claim 34 wherein the policy information is maintained in a local registry.”), [0064] (“Rules can also be set for a user or machine locally and maintained in the local system registry, *e.g.*, under HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER.”) (emphasis added to both).) The “registry” was (and remains) a well-known and routine and conventional feature of computer systems, especially Microsoft-Windows-based computing devices. (*See, e.g.*, EX1017 (Microsoft Computer Dictionary (5th ed. 2002)), pp.0011-0012 (entry for “registry” describing “A central hierarchical database in Windows 9x, Windows CE, Windows NT, and Windows 2000 used to store information necessary to configure the system

for one or more users, applications, and hardware devices.”); *see also id.*, p.009 (entry for “HKEY” describing “[s]hort for **h**key handle. In Windows 9x, Windows NT, and Windows 2000, a handle to a Registry key in which configuration information is stored.”).) The registry is a computing device’s central repository for storing configuration information, such as for users and applications. (*Id.*, p.0011.) The information in the registry can be edited using an application called the “registry editor,” also known by the name “REGEDIT.” (*See, e.g., id.*, p.0012 (entry for “Registry Editor” describing “[a]n application under Windows that allows the user to edit the entries in the registry. *Acronym:* REGEDIT”).) The registry is a **“protected data store”** because, first, the registry editor provides a structured, controlled way to access and edit data in the registry; and second, use of the registry editor itself can be restricted, thereby preventing access to the registry and protecting its contents. Lambert describes, for example, how “the administrator can...disallow the registry editor from running at all.” (Lambert, [0062]; *see also id.*, [0082] (showing “Disallowed” for the path “%WINDIR%\system32\regedit.exe”).) And therefore, by preventing the registry editor (REGEDIT or regedit.exe) from running, alteration or deletion of the **“owner control information”** is prevented based on authenticating the administrator’s credentials—thereby disclosing **“storing, by the electronic device, the owner control information in a protected data store to**

**prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information” as claimed.**

**Obviousness Over Lambert in View of Windows Guidelines Book**

134. As discussed above, Lambert alone discloses that restriction policy rules “can also be set for a user or machine locally and maintained in the local system registry, e.g., under HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER.” (Lambert, [0064].) It would have been obvious to store Lambert’s policy rules in the HKEY\_LOCAL\_MACHINE registry of the Windows operating system of a user computer and to make the policy rule information password protected, such that it could only be “**alter[ed] or delet[ed] ... in response to authenticating the owner control information using the owner information,**” in light of *The Windows Interface Guidelines for Software Design* (1995) (EX1010).

135. The Windows Guidelines Book discloses that the HKEY\_LOCAL\_MACHINE register disclosed by Lambert can be used to “add your service to the Passwords object[.]” (Windows Guidelines Book, p.007.) For example, the Windows Guidelines Book discloses the following structure of the HKEY\_LOCAL\_MACHINE register:

HKEY\_LOCAL\_MACHINE  
System  
CurrentControlSet  
Control  
PwdProvider  
*Provider Name Value Name = Value*

(*Id.*) The Windows Guidelines Book further discloses that “[t]he Passwords object in Control Panel supplies a property sheet that allows the user to set security options and manage passwords for all password-protected services in the system.” (*Id.*, p.006.) The Windows Guidelines Book indicates that adding a service to the Passwords object leads to that service being password-protected, with the user able to “change the password for the service by selecting the name and filling in the resulting dialog box.” (*Id.*, p.007.)

136. It would have been obvious to a POSITA for an administrator to store Lambert’s restriction policy rules in the Passwords object of HKEY\_LOCAL\_MACHINE to prevent alteration or deletion of the policy rule information by anyone other than an administrator. The combined system would “stor[e], by the electronic device, the owner control information [restriction policy rules] in a protected data store [the Passwords object in HKEY\_LOCAL\_MACHINE] to prevent alteration or deletion of the owner control information in response to authenticating the owner control

**information using the owner information** [e.g., administrator credentials].”

137. Lambert and the Windows Guidelines Book are analogous references. Lambert discloses that its system can be implemented on a Windows operating system, and the Windows Guidelines Book provides details about the Windows operating system. (Lambert, [0038] (describing “[w]hen a user logs on to a secure machine or network (such as one running the Windows® 2000 operating system) and is authenticated”), [0037] (discussing that its system can be “accomplished with an operating system (e.g., Microsoft Corporation’s Windows® 2000) security model”); *see also id.*, [0082]; Windows Guidelines Book, p.003 (describing the book as “an indispensable guide to designing software that runs with the Microsoft® Windows® operating system”).) Further, both Lambert and the Windows Guidelines Book relate to security and user access restriction features of computers. (Lambert, [0002] (“The present invention is generally directed to computer systems, and more particularly to an improved security framework for computer systems.”); Windows Guidelines Book, p.007 (“You can also add a page to the property sheet of the Passwords object to support other security-related services that the user can set as property values.”).) Additionally, both Lambert and the Windows Guidelines Book disclose log-in procedures and user credential-based access policies for a computer. (Lambert, [0006], [0039], [0048], [0100]; Windows Guideline Book,

pp.006-007.)

138. The Windows Guidelines Book is also analogous to the '571 patent. They relate to user access restrictions. ('571, 1:41-43 (“This system relates generally to electronic devices, and in particular to controlling application installation of such devices by a device owner.”), 1:67-2:4; Windows Guidelines Book, pp.006-007 (describing password-protected computer services).) Further, both invoke or use preexisting Microsoft software. ('571, 2:54-61 (Microsoft Exchange Server and Microsoft Outlook); Windows Guidelines Book, p.003.)

139. A POSITA would have been motivated to combine Lambert with the Windows Guidelines Book for implementation details as to how to implement Lambert's restriction policy rules that can be changed by administrators but not by end users. As discussed above, Lambert discloses that its restriction policy rules are stored on user computer terminals. (Lambert, Abstract, [0056], [0079], [0064], [0008], [0055].) Further, Lambert discloses that only users with certain privileges (e.g., administrators) are allowed to modify these rules. (*Id.*, [0057] (“the user interface provides an option that determines exactly who can specify which publishers are trusted, e.g., a domain administrator, any administrator, and/or an end user, with any higher-level administrator able to block those below from changed the setting”), [0100] (“Note that instead of restricting (or completely denying)

access, a dialog box or the like may be provided to allow a user to override the decision, possibly requiring more powerful (e.g., administrator-level) credentials.”), [0080], [0099]; *see also id.*, [0006].) The Windows Guidelines Book provides a way of storing restriction policy rules on a user computer while restricting their modification—*i.e.*, password-protecting information stored in the HKEY\_LOCAL\_MACHINE register.

140. A POSITA would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques without undue experimentation. The Lambert and Windows Guidelines Book combination is standard computing technology. For example, the Windows Guidelines Book was published in 1995, which indicates that the HKEY\_LOCAL\_MACHINE register and the use of password protection for information in that register substantially predated the '571 patent. The proposed combination would have involved nothing more than the routine implementation of known techniques.

**(g) “receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 1[d])**

141. It is my opinion that claim 1[d] is disclosed by or would have been obvious based on Lambert in at least two independent ways.

142. Lambert discloses receiving requests to access the local memory from applications running on a device. For example, Lambert discloses applications “requesting that an attachment be opened”; requesting “read/write access to a file object”; and requesting permission from an enforcement mechanism **518** for various functions, including “a create process function, a load library (e.g., a dynamic link library) function, a shell execute function, an object creation function (e.g., CoCreateInstance), script running functions and software installer functions.” (Lambert, [0010], [0042], [0072]; *see also id.*, [0014], [0038] (“computing tasks are performed by accessing the system or network’s resources via processes”), [0056] (“whenever a request to open that file is received, a hash of the file matches the saved hash and rule”), [0038], [0043], [0046], [0048], [0066], [0070], [0076].) These requests represent requests to “**access local memory**” since they involve accessing items stored in the local memory, including applications and other files. (*Id.*, [0082] (showing applications in local “windir” and “programfiles” directories), [0063] (discussing software in a “local machine (e.g., My Computer)” zone); *see also id.*, Fig. 1 (showing “Application Programs” and “Program Data” in “System Memory (ROM) **131**”).) Further, Lambert discloses that application execution involves accessing the computer’s local random-access memory (RAM). (*Id.*, [0031] (“RAM **132** typically contains data and/or program modules that are ... presently being

operated on by processing unit 120.”), Fig. 1.)

### **Figure 5A Embodiment**

143. For example, Lambert discloses that a software application **510** requests use of the computer’s resources for a certain process—including opening, loading, or executing the application located in memory. (Lambert, [0066]; *see also id.*, [0072], [0042] (“the process **300** specifies the type of access it desires (e.g., obtain read/write access to a file object)”), [0038] (“An access token is associated with each process of the user, whereby anytime a process requests to do work on behalf of the user, the access token can be first checked to see if the process has the appropriate rights and/or privileges to do what is being requested, such as access a resource.”).) This is shown in Figure 5A of Lambert, reproduced below, where “a process **508** such as a process of a user or application [is] requesting to open a software file **510**”:

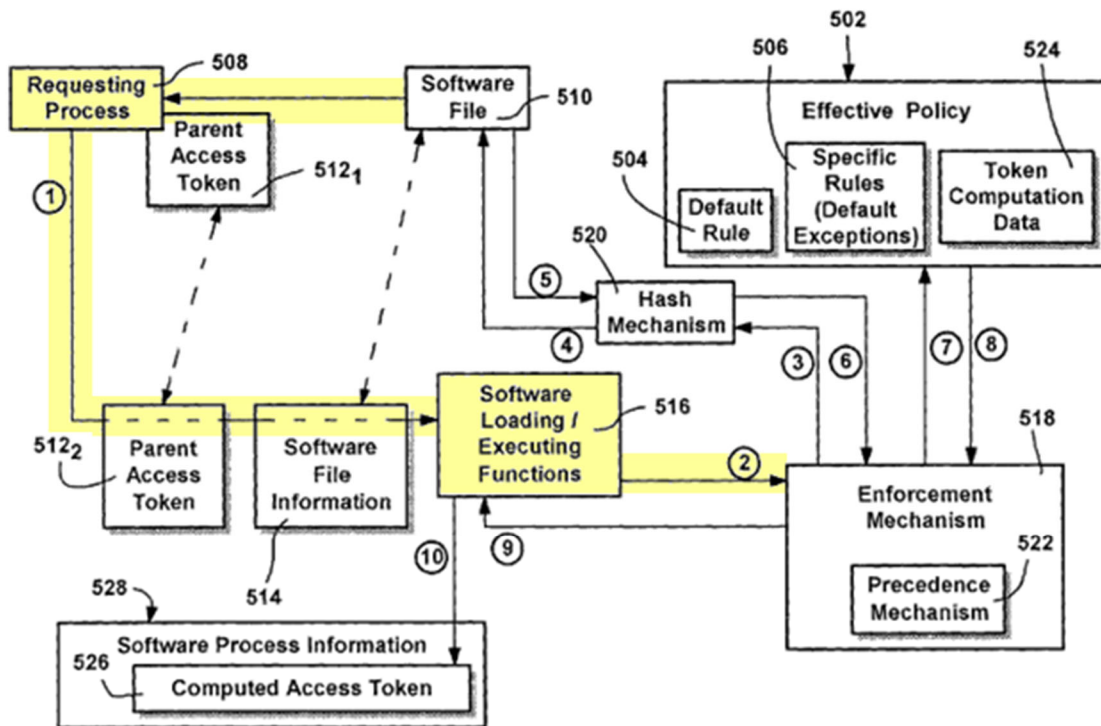


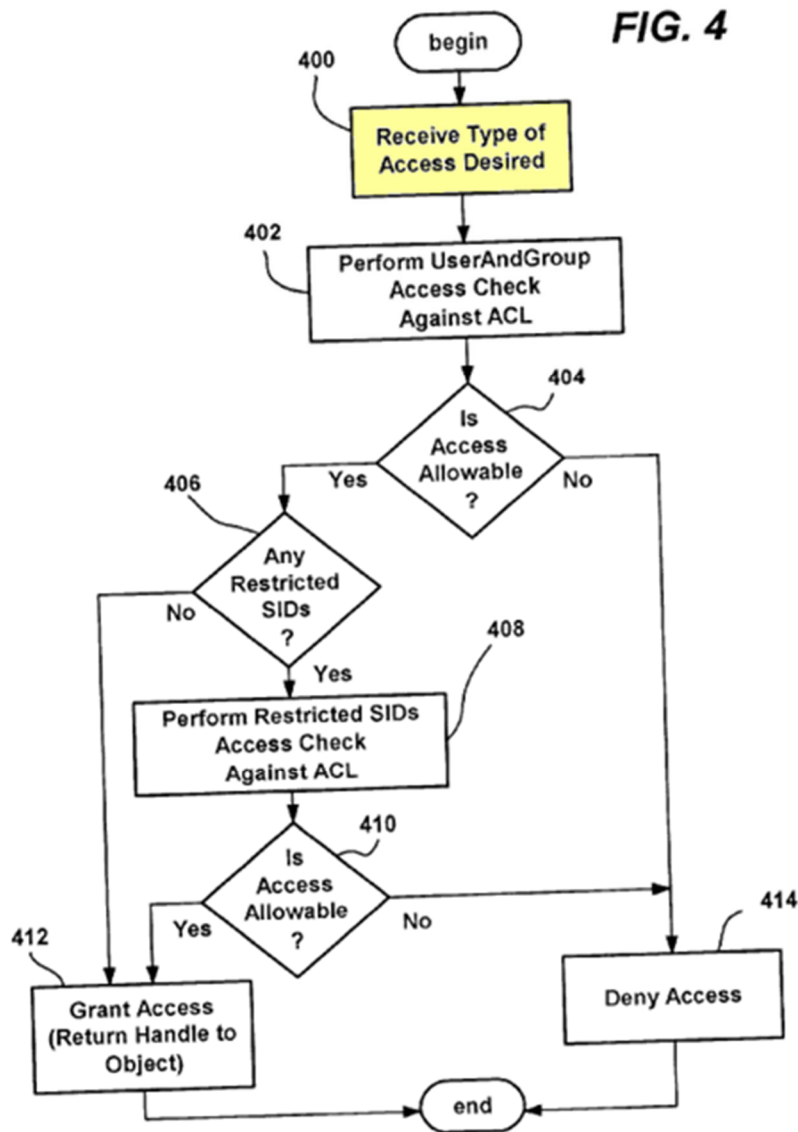
FIG. 5A

(*Id.*, Fig. 5A (color added), [0066].) Lambert discloses that software can be stored and executed via the local memory. (*Id.*, [0082] (showing applications in local “windir” and “programfiles” directories), [0063] (discussing software in a “local machine (e.g., My Computer)” zone), [0031] (“RAM 132 typically contains data and/or program modules that are ... presently being operated on by processing unit 120.”), Fig. 1; *see also id.*, Fig. 1 (showing “Application Programs” and “Program Data” in “System Memory (ROM) 131”).) The arrow labeled with the circled numeral one (1) “generally represents such a call from the requesting process 508 to the one of the functions of the set 516.” (*Id.*, [0066].) Further, circled numeral two

(2) represents “each of the functions **516** ... provid[ing] the software file information **514** to an enforcement mechanism” as part of the requesting process. (*Id.*, [0067].) Through this process, Lambert discloses “**receiving, by the electronic device, from an application operating on the electronic device** [*e.g.*, software application **510**], **a request to access local memory on the electronic device** [*e.g.*, executing of software functions, including loading or executing software via the local memory].”

### **Restricted Token Disclosures**

144. Lambert also discloses that the enforcement mechanism discussed above can associate a restricted access token with an application. (Lambert, [0070] (“the enforcement mechanism **518** can compute and associate a restricted token with the software file **510**”), [0071], [0074], [0100], [0013]-[0014], Figs. 2, 3, 9; *see also id.*, [0037]-[0043].) Then, when the application seeks to execute a process (*e.g.*, gain read or write access to another file), the application may “**request to access local memory on the electronic device**”—*e.g.*, the permissions indicated by the restricted token are compared against permissions associated with a target file. (*Id.*, [0048] (disclosing a “security mechanism **308** to compare the user and group security IDs listed in the restricted token **210**”), [0042].) For example, Lambert discloses that step **400** in Figure 4 represents “requesting access to the object **302**,” which can be a “file object” in local memory. (*Id.*, [0048], [0042].)



(*Id.*, Fig. 4 (highlighting added).) This step **400** represents a further level at which Lambert discloses “**receiving, by the electronic device, from an application operating on the electronic device [i.e., an application associated with a restricted token], a request to access local memory on the electronic device [e.g., a request for read/write access to a file object stored in local memory].**”

- (h) **“determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 1[e])**

145. It is my opinion that claim 1[e] is disclosed by or would have been obvious based on Lambert in multiple ways. The **“owner control information”** portion of this element is discussed above. The **“permission associated with the application in the owner control information”** is also addressed above.

146. Lambert discloses that its system determines whether or not the local memory access requested by an application discussed above is allowed to move forward based on the application-by-application policy rules provided by an administrator. For example, Lambert discloses that “the present invention provides an improved computer security system and method wherein software that possibly includes executable code is identified and classified, and then a rule corresponding to the classification (or if none correspond, a default rule) automatically and transparently determines the software’s ability to execute.” (Lambert, [0008] (emphasis added); *see also id.*, [0052] (disclosing “a method and system that determines access to resources based on an identification (classification) of software that may contain executable content”), [0067] (“the enforcement mechanism consults the effective policy **502** to determine which rule applies for the file **510**, and from the rule determines whether to open/execute the file, and if so, the extent of

any restricted execution context for the file **510**”), [0013] (“The security level determines whether the software can run, and if so, the execution environment in which it will run.” (emphasis added)), [0014] (disclosing “a restricted access token that restricts the software to an extent that corresponds to the security level determined by the rule”).) Since Lambert discloses applications can be stored in local memory, this “**determining**” process represents whether “**access [to] the local memory**” is allowed. (*Id.*, [0082] (showing applications in local “windir” and “programfiles” directories), [0063] (discussing software in a “local machine (e.g., My Computer)” zone); *see also id.*, Fig. 1 (showing “Application Programs” and “Program Data” in “System Memory (ROM) **131**”).) Further, Lambert discloses that application execution involves accessing the computer’s local random-access memory (RAM). (*Id.*, [0031] (“RAM **132** typically contains data and/or program modules that are ... presently being operated on by processing unit **120**.”), Fig. 1.)

### **Figure 5A Embodiment**

147. For example, Lambert discloses that an access request from an application **510** leads to a query to an “enforcement mechanism **518**,” which “obtains a security level indicative of whether the file **510** can be executed, and if so, the extent of any restricted execution context for any processes of the file **510**.” (Lambert, [0069]; *see also id.*, [0070]-[0072].) This determination of the

enforcement mechanism **518** is based on policy rules input by the administrator. (*Id.*, [0067], [0062], [0064].) This enforcement mechanism is shown in Figure 5A, reproduced below:

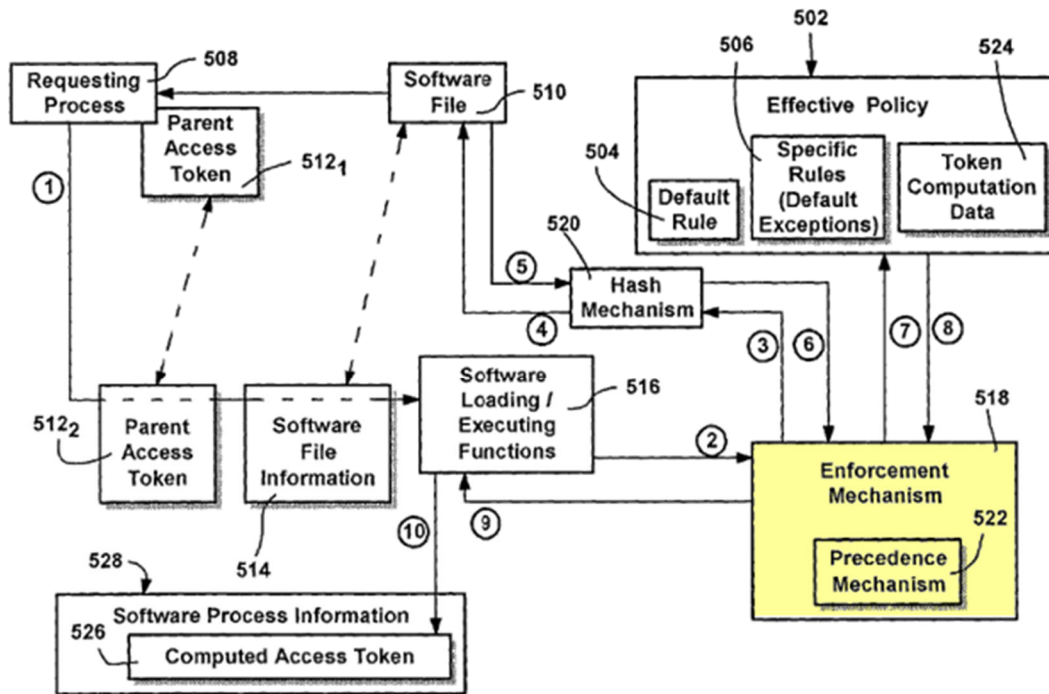


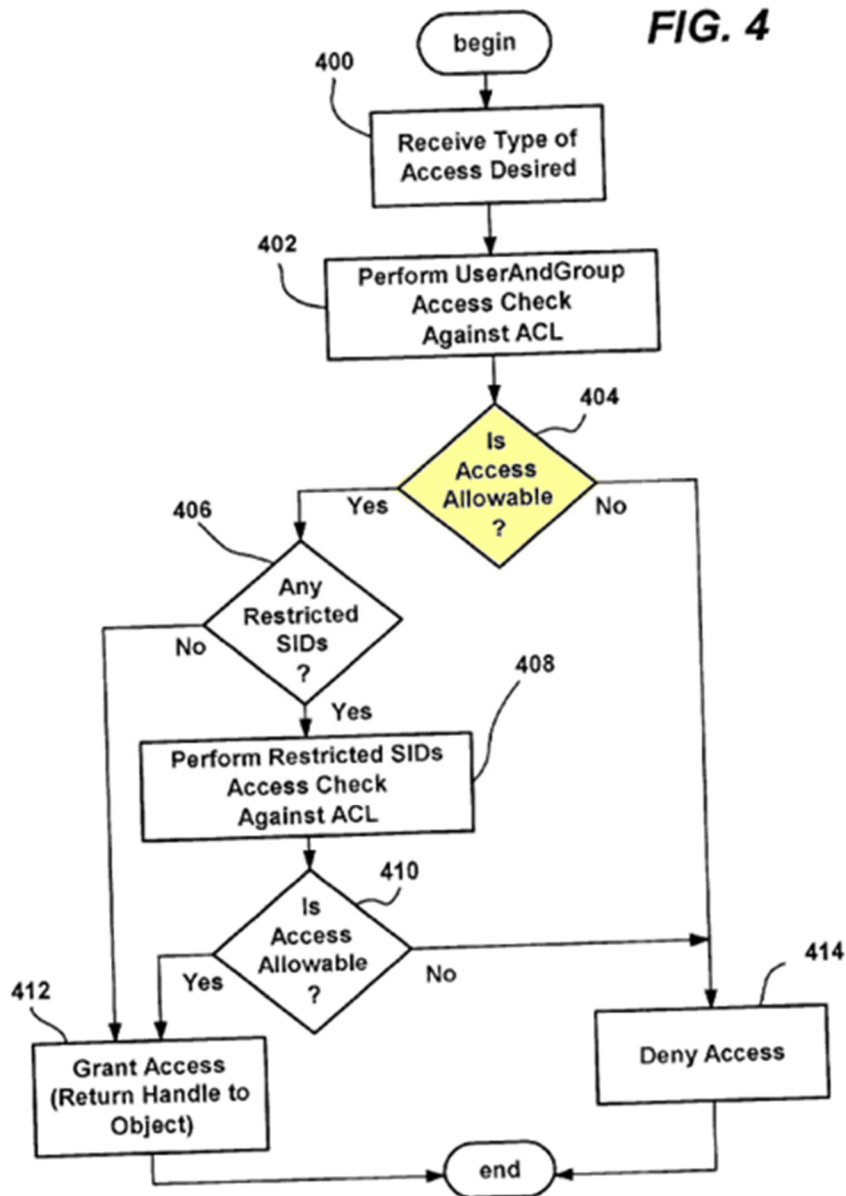
**FIG. 5A**

(*Id.*, Fig. 5A (color added).)

148. Thus, Lambert discloses “**determining whether the application is allowed to access the local memory** [e.g., whether application can execute, when the application is stored or executed via local memory] **in response to identifying a permission associated with the application in the owner control information** [e.g., administrator policy information].”

### Restricted Token Disclosures

149. Further, if the policy rules lead to the enforcement mechanism associating a restricted token with an application, Lambert discloses that its system determines application access based on the application's restricted token when it requests access to an object in local memory—*e.g.*, read/write access to a file object. (Lambert, [0070], [0071], [0074], [0100], [0013]-[0014], Figs. 2, 3, 9; *see also id.*, [0037]-[0043].) This step is shown as element **404** in Figure 4:



(*Id.*, Fig. 4 (color added), [0049], [0048].)

150. Accordingly, the process of determining whether an application with a restricted access token can access a target object represents another level at which Lambert discloses “**determining whether the application is allowed to access the**

**local memory** [e.g., read/write access to a file object] **in response to identifying a permission associated with the application in the owner control information** [e.g., a restricted access token derived by the enforcement mechanism from administrator policy rules].”

**(i) “controlling application access to the local memory based upon the determining.” (Claim 1[f])**

151. It is my opinion that claim 1[f] is disclosed by or would have been obvious based on Lambert in multiple ways.

152. As explained above, Lambert teaches “**controlling application access.**” For example, Lambert discloses that “the present invention automatically controls whether content is executable, and if so, the extent (if any) to which it is restricted.” (Lambert, [0054] (emphasis added); *see also id.*, Abstract (“A system and method that automatically, transparently and securely controls software execution by identifying and classifying software, and locating a rule and associated security level for executing executable software.”), [0101] (describing invention as “a framework that controls the execution of software in accordance with a restriction policy”), [0050] (“The design of restricted tokens provides for significant flexibility and granularity within the context of a user to control what different processes are allowed to do.” (emphasis added)), [0052] (“by allowing the administrator to set a default rule, an administrator can efficiently control software in any environment”

(emphasis added)), [0022] (describing “controlling software execution in accordance with one aspect of the present invention” (emphasis added)), [0058] (describing “using conventional access control technology, such as via discretionary access control lists”), [0008] (describing invention as “an improved computer security system and method”).) This involves “**controlling application access to local memory**” since it involves accessing items stored in the local memory, including applications and other files. (*Id.*, [0082] (showing applications in local “windir” and “programfiles” directories), [0063] (discussing software in a “local machine (e.g., My Computer)” zone); *see also id.*, Fig. 1 (showing “Application Programs” and “Program Data” in “System Memory (ROM) **131**”).) Further, Lambert discloses that application execution involves accessing the computer’s local random-access memory (RAM). (*Id.*, [0031] (“RAM **132** typically contains data and/or program modules that are ... presently being operated on by processing unit **120**.”), Fig. 1.)

### **Figure 5A Embodiment**

153. For example, Lambert discloses that based on the above determining step discussed regarding the Figure 5A embodiment, its system “**control[s] application access to the local memory based upon the determining.**” For example, Lambert discloses that in step (9), the enforcement mechanism **518**

“completes the call and returns information back to the software function **516** that called it, the returned information essentially including an instruction on whether to open the file, and if so, the token to associate with the file.” (Lambert, [0071].) Further, in step (10), Lambert discloses that “[t]he returned token ... is maintained in a set of process information **528** (e.g., in a protected location) associated with that file, as generally represented in FIG. 5A by the arrow labeled ten (10).” (*Id.* (“If the computed token **526** is a restricted token, the process of the software file can now execute, but only in association with the restricted token, thus providing the rule-determined secure execution environment.”).) Steps (9) and (10) are shown in Figure 5A below:

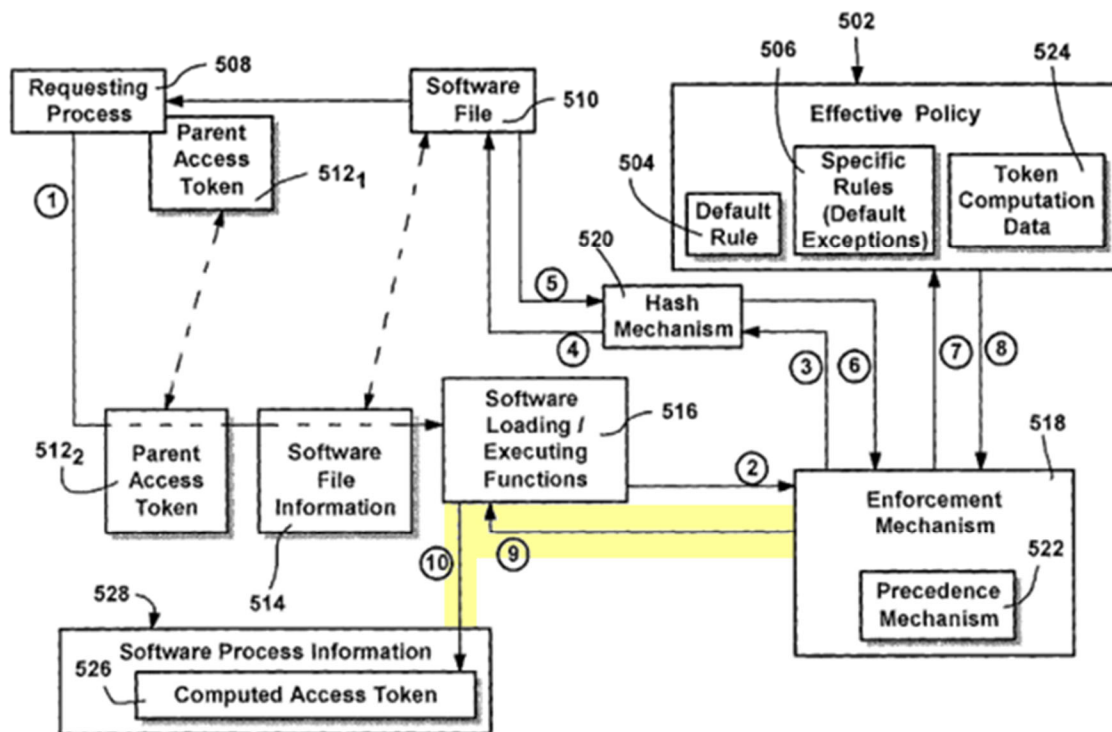


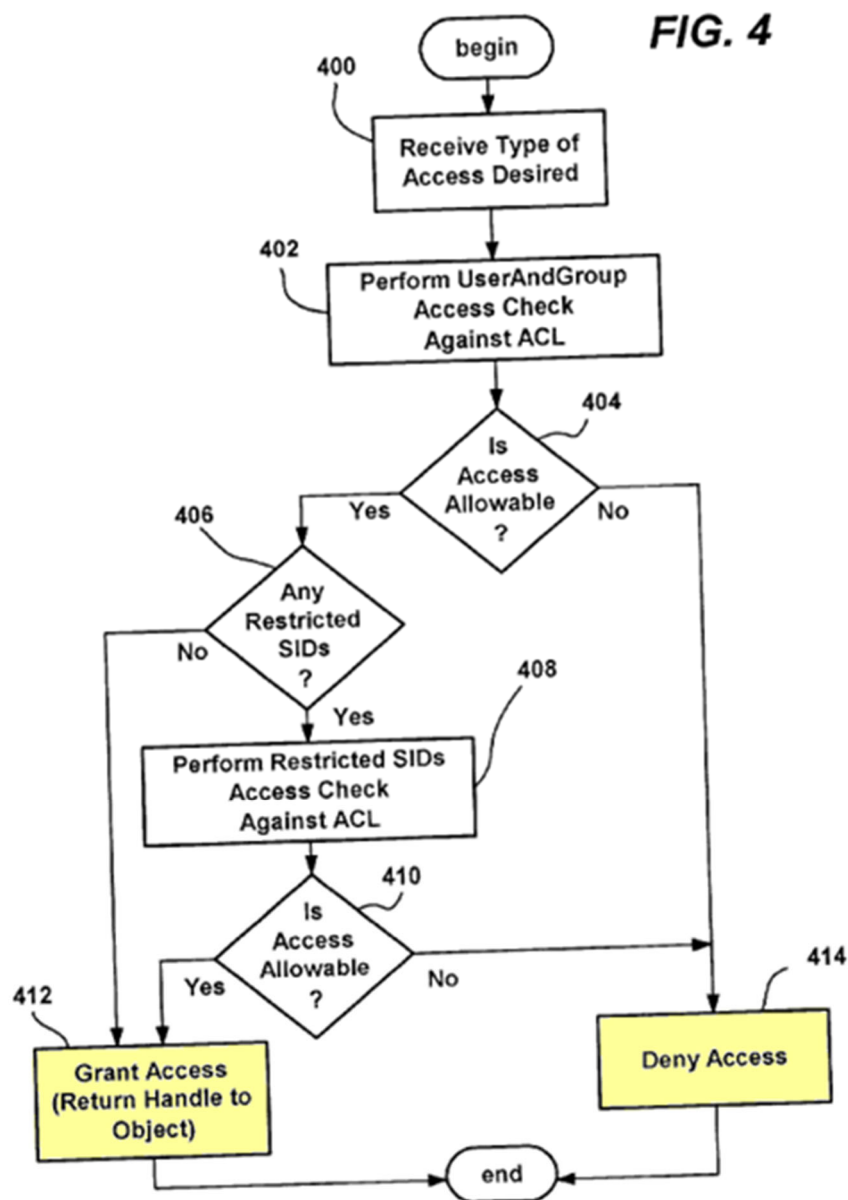
FIG. 5A

(*Id.*, Fig. 5A (highlighting added), [0071].) Lambert is thus teaching or rendering obvious “**controlling application access to the local memory based upon the determining**” step, since it discloses controlling whether an application can run (e.g., an application stored and executing via local memory) and, if so, in what restricted capacity using the enforcement mechanism **518**.

### Restricted Token Disclosures

154. Further, Lambert discloses controlling application access to the local memory based on the restricted token associated with the application via the enforcement mechanism process. (Lambert, [0071].) Lambert discloses that based

on the determining step discussed above related to Lambert's restricted token control process, access to a target object (e.g., read/write access to a file object) is either granted or denied. (*Id.*, [0049]; *see also id.*, [0043]-[0048].) This is shown in Figure 4 below:



(*Id.*, Fig. 4 (color added).)

155. Thus, in its disclosures regarding restricted tokens, Lambert discloses a further level at which its system “**control[s] application access to the local memory** [*e.g.*, read/write access to a file stored in local memory] **based upon the determining.**”

156. It is thus my opinion that claim 1 is disclosed by or obvious in light of Lambert (Ground 1). Alternatively, claim 1 is obvious in view of Lambert, Frank, Gomberg, and Windows Guidelines Book (Ground 2).

## 2. Dependent claim 2

157. For reference, claim 2 recites:

2. The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

(’571, 29:30-32 (Claim 2).)

158. It is my opinion that claim 2 is disclosed by or obvious in light of Lambert. Claim 2 is satisfied by both Grounds 1 and 2.

159. As discussed for claim 1[d], the “**request to access the local memory**” in Lambert includes a request by an application running on the device to access an object in local memory, such as a file. (Lambert, [0042], [0066].)

160. With respect to that “**request**” “**compris[ing] a request to erase data**

**from the local memory,”** Lambert further discloses the request by the application can include “the type of access it desires (e.g., obtain read/write access to a file object)[.]” (Lambert, [0042].) In response, the operating system provides a restricted token, which is compared against a “discretionary access control list (DACL) **312**” for the file object. (*Id.*, [0043].) This DACL contains access control entries, where each entry includes “access rights in the form of a bitmask wherein each bit corresponds to a permission (e.g., one bit for write access, and so on).” (*Id.*) Based on the comparison, the access request is either allowed or denied. (*Id.*; *see also id.*, [0014] (“If allowed but restricted, the returned restricted token is associated with the code’s processes, constraining the code accordingly.”).) In the case of a request for write access, a POSITA would have understood and found it obvious that a request for write access would logically also be “**a request to erase data,**” because providing the ability to write data provides the ability to erase data. This is because in order to actually erase data from memory, that data is typically overwritten (usually with zeroes or meaningless text), and having write access provides that ability to overwrite. For example, the Microsoft Computer Dictionary (5th ed. 2002) (EX1017), defines “erase” as “[t]o remove data permanently from a storage medium. This is usually done by replacing existing data with zeroes or meaningless text, or in magnetic media, by disturbing the magnetic particles’ physical arrangement,

either with the erase head or with a large magnet.” (*Id.*, p.008 (entry for “erase”) (emphasis added); *see also id.*, p.0014 (entry for “write mode” stating that “[i]n computer operation, the state in which a program can write (record) information in a file. In write mode, the program is permitted to make changes to existing information.” (emphasis added)), p.0010 (defining “read-only” as “[c]apable of being retrieved (read) but not changed (written). A read-only file or document can be displayed or printed but not altered in any way.”).)

161. Lambert also discloses that its system can prevent users from having “write access to the system directory, ... since these programs are needed for normal system operation.” (Lambert, [0061].) Such a rule indicates that any requests to **“erase data from the local memory”** in that directory are prohibited, as enforced by Lambert’s system as shown, for example, in Figure 5A. (*Id.*, [0065] (indicating that the effective policy **502** enforced by the system includes “specific rule[] **506**”); *see also id.*, claim 39 (“wherein the folder is protected from write access with respect to a user executing the software”).)

162. Accordingly, it is my opinion that Lambert discloses **“the request to access the local memory comprises a request to erase data from the local memory.”**

**3. Dependent claim 3**

163. For reference, claim 3 recites:

3. The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

(’571, 29:33-35 (Claim 3).)

164. It is my opinion that claim 3 is disclosed by or obvious in light of Lambert. Claim 3 is satisfied by both Grounds 1 and 2.

165. As discussed above for claim 1[d] and claim 2, Lambert discloses that its system can receive a request from a process “desir[ing] access to an object **302**,” including “the type of access it desires (e.g., obtain read/write access to a file object)[.]” (Lambert, [0042] (emphasis added).) Such “read” and “write” access is a routine and conventional feature of data access in computer systems. (EX1017 (Microsoft Computer Dictionary (5th ed. 2002)), pp.0010 (defining “read-only” as “[c]apable of being retrieved (read) but not changed (written). A read-only file or document can be displayed or printed but not altered in any way.”), 0014 (entry for “write mode” stating that “[i]n computer operation, the state in which a program can write (record) information in a file. In write mode, the program is permitted to make changes to existing information.”).) As explained above, Lambert explains that, based on a comparison against an access control list having information about access

permissions (such as write access), the access request is either allowed or denied. (Lambert, [0042], [0043].) Therefore, because Lambert discloses that a request for access to a resource can comprise a request for “read” access, Lambert discloses that its system manages and enforces access restrictions where **“the request to access the local memory comprises a request to read data from the local memory”**—*e.g.*, to read a file stored in local memory.

166. Accordingly, it is my opinion that Lambert discloses **“the request to access the local memory comprises a request to read data from the local memory.”**

#### **4. Dependent claim 4**

167. For reference, claim 4 recites:

4. The method of claim 1, further comprising restricting modification of the owner control information after the owner control information has been stored in the protected data store.

(’571, 29:36-39 (Claim 4).)

168. It is my opinion that claim 4 is disclosed by or obvious in light of Lambert. Claim 4 is satisfied by both Grounds 1 and 2.

169. Lambert discloses **“restricting modification of the owner control information after the owner control information has been stored in the protected data store.”** As explained above for claim 1[c], Lambert discloses a user

interface program for adjusting policy rules that can only be accessed with administrator privileges and other privilege-based restrictions on changing policy rules, thereby “**restricting modification.**”. (Lambert, [0081], [0078], [0039], [0057], [0100], [0080], [0099], [0064].) Further, Lambert discloses that locally stored policy settings could be stored in the “registry” of a user computer, which constitutes a “**protected data store**” for which modification can be “**restrict**[ed].” (*Id.*, claim 37, [0064], [0062], [0082]; EX1017 (Microsoft Computer Dictionary (5th ed. 2002)), pp.0011-0012, 009.)

170. As discussed above for claim 1[c], it would also have been obvious to a POSITA over Lambert in view of the Windows Guidelines Book to store policy information (“**owner control information**”) in the HKEY\_LOCAL\_MACHINE register and make that information password protected such that only an administrator could access or change it. Accordingly, Lambert and the Windows Guidelines Book render obvious “**restricting modification** [*i.e.*, preventing non-administrator alteration] **of the owner control information after the owner control information has been stored in the protected data store.**”

## 5. Dependent claim 5

171. For reference, claim 5 recites:

5. The method of claim 1, wherein the owner control information includes an authorization record and an application identifier for

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

each of the applications, and the owner control information is provided by an external source through a wireless communication channel.

('571, 29:40-44 (Claim 5).)

172. It is my opinion that claim 5 is disclosed by or obvious in light of Lambert. Claim 5 is satisfied by both Grounds 1 and 2.

173. Lambert discloses that the “**owner control information includes an authorization record and an application identifier for each of the applications.**”

As I explained above, Lambert discloses an example of a policy, with each row listing a rule:

|                                       |                                                   |                          |                           |                          |                                                           |                         |                                      |              |               |
|---------------------------------------|---------------------------------------------------|--------------------------|---------------------------|--------------------------|-----------------------------------------------------------|-------------------------|--------------------------------------|--------------|---------------|
| OnlySignedLockDown Path               | HKCU<br>%windir%                                  | Disabled<br>Unrestricted | CP only<br>All file types | Path                     | %programfiles%\micro-soft\office\office\powerpoint.exe    | Disabled                | <exact match>                        |              |               |
| Certificate Explorer- byLockDown Path | <publisher cert><br>HKCU                          | Unrestricted<br>Disabled | CP only                   | Path                     | %programfiles%\micro-soft\office\office\frontpg.exe       | Disabled                | <exact match>                        |              |               |
| Path                                  | %programfiles%\Internet Explorer\                 | Unrestricted             | All file types            | Path                     | %programfiles%\micro-soft\office\office\outlook.exe       | Disabled                | <exact match>                        |              |               |
| WMPOnlyLockDown                       | HKCU                                              | Disabled                 | CP                        | NoAttachments-LockAll    | HKCU                                                      | Unrestricted            | CP/LL                                |              |               |
| Path                                  | %windir%                                          | Unrestricted             | All file types            | Path                     | %USERPROFILES%\local settings\tempory internet files\OLK* | Disabled                | All file types                       |              |               |
| Path                                  | %programfiles%\Windows Media Player               | Unrestricted             | All file types            |                          |                                                           |                         |                                      |              |               |
| PFNoMediaLockDown                     | HKCU                                              | Disabled                 | CP                        | DangerousApps\lock       | HKCU                                                      | Unrestricted            | CP                                   |              |               |
| Path                                  | %windir%                                          | Unrestricted             | Only All file types       | Hash                     | Regedit.exe                                               | Disabled                | N/A                                  |              |               |
| Path                                  | %programfiles%\                                   | Unrestricted             | All file types            | Hash                     | Regedit32.exe                                             | Disabled                | N/A                                  |              |               |
| Path                                  | %programfiles%\                                   | Unrestricted             | All file types            | Hash                     | cmd.exe                                                   | Disabled                | N/A                                  |              |               |
| Path                                  | %programfiles%\                                   | Unrestricted             | All file types            | Path                     | %WINDIR%\system32\cmd.exe                                 | Disabled                | <exact match>                        |              |               |
| Path                                  | %programfiles%\Windows Media Player wmpplayer.exe | Disabled                 | All file types            | Path                     | %WINDIR%\system32\regedit.exe                             | Disabled                | <exact match>                        |              |               |
| Hash OfficeAllowLock-AllDown Path     | HKCU                                              | Disabled                 | N/A                       | Path                     | %WINDIR%\system32\regedit32.exe                           | Disabled                | <exact match>                        |              |               |
| Path                                  | %windir%                                          | Unrestricted             | All file types            | InnocuousLockAll-Machine | HKLM                                                      | Unrestricted            | CP/LL                                |              |               |
| Path                                  | %programfiles%\micro-soft\office                  | Unrestricted             | All file types            | Path                     | %windir%\system32\GDH32.DLL                               | Unrestricted            | <exact match>                        |              |               |
| OfficeWordOnly-LockAllDown Path       | HKCU                                              | Disabled                 | CP/LL                     | Path                     | %windir%\system32\ntdll.dll                               | Unrestricted            | <exact match>                        |              |               |
| Path                                  | %programfiles%\micro-soft\office\office\excel.exe | Disabled                 | <exact match>             | Hash                     | %windir%\system32\shell32.dll                             | Unrestricted            | <exact match>                        |              |               |
|                                       |                                                   |                          |                           |                          |                                                           | Hash                    | %windir%\system32\kernel32.dll       | Unrestricted | <exact match> |
|                                       |                                                   |                          |                           |                          |                                                           | No VBS Path             | %WINDIR%\system32\scrnrd.dll         | Unrestricted | CP/LL         |
|                                       |                                                   |                          |                           |                          |                                                           | Path                    | %WINDIR%\system32\crypt.exe          | Disabled     | <exact match> |
|                                       |                                                   |                          |                           |                          |                                                           | Trusted Publishers\Lock | HKCU, only admins can add publishers | Unrestricted | CP            |
|                                       |                                                   |                          |                           |                          |                                                           | Certificate             | Stock ticker publisher               | Unrestricted |               |
|                                       |                                                   |                          |                           |                          |                                                           | Certificate             | xenroll publisher                    | Unrestricted |               |
|                                       |                                                   |                          |                           |                          |                                                           | Certificate             | MSNBC news publisher                 | Unrestricted |               |

(Lambert, [0082].) A larger excerpt of [0082] is reproduced here:

|                                                  |                                         |                                            |                                 |
|--------------------------------------------------|-----------------------------------------|--------------------------------------------|---------------------------------|
| OnlySignedLockDown<br>Path                       | HKCU<br>%windir%                        | Disallowed<br>Unrestricted                 | CP only<br>All file<br>types    |
| Certificate<br>IexploreOn-<br>lyLockDown<br>Path | <publisher cert><br>HKCU<br>%windir%    | Unrestricted<br>Disallowed<br>Unrestricted | CP only<br>All file<br>types    |
| Path                                             | %programfiles%\Internet<br>Explorer\    | Unrestricted                               | All file<br>types               |
| WMPOnlyLockDown<br>Path                          | HKCU<br>%windir%                        | Disallowed<br>Unrestricted                 | CP<br>Only<br>All file<br>types |
| Path                                             | %programfiles%\<br>Windows Media Player | Unrestricted                               | All file<br>types               |
| PFNoMediaLockDown                                | HKCU                                    | Disallowed                                 | CP<br>Only                      |

(*Id.* (excerpt).) This example policy includes a list of entries for applications—for example, for the Internet Explorer application, there is an entry that specifies an associated path (i.e., “%programfiles%\Internet Explorer”) and rule (i.e., “Unrestricted All File types”). The associated rule for an application (e.g., “Disallowed,” “Unrestricted,” “All file types,” and “CP only”) is an “**authorization record**” because it specifies a level of authorization (e.g., permitted tasks) associated with the application. For example, “disallowed” means that the application is not permitted to run, while “unrestricted” means that there are no restrictions on running the application. (*Id.*, [0079] (describing “unrestricted operation,” “constrained,” “untrusted,” etc. as “authorization levels”), [0053] (disclosing “various selectable

classification criteria”), [0054], [0058]-[0063], [0068].) The associated path for an application (e.g., “%programfiles%\Internet Explorer”) is an “**application identifier**” because, as Lambert explains, it identifies the application. (*Id.*, [0053] (“To identify and classify software, (e.g., maintained in a file), various selectable classification criteria are made available to an administrator, including a unique hash value of the file’s content (e.g., via an MD5 image hash), and whether the file is digitally signed, and if so, by what entity. Other criteria for classifying software includes the software’s file system or network path, and/or its origin or source, e.g., its URL (Uniform Resource Locator) zone.” (emphasis added)), [0058] (“Another rule that can be applied to software is based on identifying and classifying a file by the specific folder it is in, or based on its fully qualified path.” (emphasis added)).)

174. Lambert also discloses that a policy can include rules based on the unique hash value of an application, “with the rule specifying whether (and if so, how) a software file having that hash value will execute.” (Lambert, [0056].) Lambert explains that a hash value is “essentially a fingerprint that uniquely identifies a file regardless of whether the file is moved or renamed.” (*Id.*, [0055].) Lambert indicates that when there is a hash rule for an application in an administrator policy, “a hash rule can specify how it will be executed, e.g., unrestricted (normal) or restricted (and to what extent).” (*Id.*, [0056].) Hash rules for applications are

disclosed in the table provided in paragraph [0082] of Lambert—for example, the following:

|      |              |            |     |
|------|--------------|------------|-----|
| Hash | Regedit.exe  | Disallowed | N/A |
| Hash | Regedt32.exe | Disallowed | N/A |
| Hash | cmd.exe      | Disallowed | N/A |

(*Id.*, [0082].) Hash rules are an example of information included in the “**owner control information**” with “**an authorization record** [*e.g.*, restrictions, including “Disallowed”] **and an application identifier** [*e.g.*, the hash value for a particular application] **for each of the applications.**”

175. Lambert discloses that the “**authorization record**” is “**provided by an external source.**” Lambert discloses that restriction policy information can be provided “within one or more group policy objects distributable over a network.” (Lambert, [0064]; *see also id.*, [0012] (“dynamically generating and distributing new policy including a rule that prevents that software from running”), [0008].) By distributing a policy over a network, the policy, including its authorization records, is provided by an “**external source.**” This is consistent with the ’571 patent which refers to internal sources, such as a device’s local, internal storage, and remote/external sources. (*E.g.*, ’571, 18:57-61 (“some or all these lists can be maintained locally within the devices owner control information store; alternatively, one or more supported lists could be maintained remotely or on an external memory

device”).)

176. Lambert discloses and renders obvious that its system can provide policy information (“**owner control information**”) “**through a wireless communication channel.**” For example, Lambert discloses that the computing devices in its system can connect to a “local area network (LAN) **171** and a wide area network (WAN) **173**,” which are “commonplace in offices, enterprise-wide computer networks, intranets and the Internet.” (Lambert, [0034]; *see also id.*, [0035].) Lambert further discloses that the computing devices can communicate by wired or wireless media, describing a general purpose computing device (**110**) having communication media that includes “wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media.” (*Id.*, [0030] (emphasis added).) By at least 2002, wireless networks, such as wireless LANs, were well known and widely used. (*See, e.g.*, EX1017 (Microsoft Computer Dictionary (5th ed. 2002)), p.0013 (entry for “wireless LAN” describing “[a] LAN (local area network) that sends and receives data via radio, infrared optical signaling, or some other technology that does not require a physical connection between individual nodes and hub. Wireless LANs are often used in office or factory settings where a user must carry a portable computer from place to place.”).) Wireless communication among devices in, for

example a wireless LAN, takes place through wireless communication channels. (See, e.g., *id.*, p.007 (entry for “channel”).) A POSITA would have therefore understood and found it obvious for Lambert’s policy information (“**owner control information**”) to be provided from a remote/external source “**through a wireless communication channel.**”

**6. Dependent claim 6**

177. For reference, claim 6 recites:

6. The method of claim 5, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

(’571, 29:45-49 (Claim 6).)

178. It is my opinion that claim 6 is disclosed by or obvious in light of Lambert. Claim 6 is satisfied by both Grounds 1 and 2.

179. Lambert discloses that the “**authorization record**” is “**provided by an external computer.**” As discussed above for claim 5, Lambert discloses that restriction policy information can be provided “within one or more group policy objects distributable over a network.” (Lambert, [0064]; *see also id.*, [0008], [0012].)

180. Lambert discloses that the “**authorization record[s]**” in policy

information (“**owner control information**”) are “**related to determining whether access to the local memory is allowed.**” For example, the rules in the administrator policy indicate whether a software application can execute at all, which is “**related to determining whether access to the local memory is allowed.**” Further, as I explained above in claim 1[e], the rules in an administrator policy like the one disclosed in Lambert’s paragraph [0082] are used to enforce what processes applications can execute. (Lambert, [0082], [0079].) Policy information can lead to a restricted token being associated with a software application or process. (*Id.*, [0072].) The restricted token is then used to determine whether a local memory request is allowed for an application—for example, a request for read/write access for a file in local memory. (*Id.*, [0042] (“When the process **300** desires access to an object **302**, the process **300** specifies the type of access it desires (e.g., obtain read/write access to a file object), and the operating system (e.g., kernel) level provides its associated token to an object manager **304.**”); *see also id.*, [0043], Figs. 1, 3.) Accordingly, Lambert discloses that its “**authorization record[s]**” are “**related to determining whether access to the local memory is allowed.**”

181. Lambert further discloses that the external computer is “**used to enforce policies for operating electronic devices within an organization.**” For example, as discussed above, Lambert discloses distributing a “group policy object

... over a network.” (Lambert, [0008].) Lambert discloses that “[i]n an enterprise environment, the policy may be set for sites, domains, organizational units, groups and/or users via group policy technology.” (*Id.*, [0012].) Further, Lambert indicates in its “Background of the Invention” section that its system is intended to address problems in the prior art related to “enterprise computing environments” and “business users.” (*Id.*, [0003] (“administrators begin to lose control over what software code the enterprise’s machines are executing”), [0007] (“In sum, in contemporary computer systems, running unknown code cannot be prevented, and indeed is necessary to an extent in many enterprises, yet doing so leads to increased support costs in system maintenance and helpdesk time, and decreased user productivity.”), *id.* (discussing the “rise in the usage of networks, email and the Internet for business computing”).) Thus, Lambert discloses using its system for “**enforc[ing] policies for operating electronic devices within an organization**”—*e.g.*, a business enterprise.

## 7. Dependent claim 7

182. For reference, claim 7 recites:

7. The method of claim 1, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

(’571, 29:50-52 (Claim 7).)

183. It is my opinion that claim 7 is disclosed by or obvious in light of Lambert. Claim 7 is satisfied by both Grounds 1 and 2.

184. As discussed for claims 5 and 6 above, Lambert discloses providing policy information (“**owner control information**”) from an external source or computer. (Lambert, [0064]; *see also id.*, [0008], [0012].) For example, as noted, Lambert describes how policy information can be provided “within one or more group policy objects distributable over a network.” (*Id.*, [0064].)

185. Lambert further discloses and renders obvious “**an update to the owner control information is provided by an external source for storage on the electronic device.**” For example, Lambert discloses that its system can “automatically generate and propagate rules, for example, by dynamically accessing a database to find new software that has been identified as having a virus, and dynamically generating and distributing new policy including a rule that prevents that software from running.” (Lambert, [0012].) This “distributing” of new policy information indicates local storage on user devices. (*Id.*, [0004] (“distributed to various computers”), [0056] (“maintained or distributed to the machine, (e.g., via a policy object)”), Abstract (“group policy object distributable over a network”).) Further, Lambert indicates that an administrator can periodically update policy information. (*Id.*, [0056] (“the hash rule for a certain file may need to be frequently

updated”).) A POSITA would have understood that, in order for the new rules to take effect, those rules, just like original policy information, would be received from the external source and stored on the electronic device. A POSITA would have therefore understood that the generation and distribution of new or updated rules constitute providing “**an update to the owner control information is provided by an external source for storage on the electronic device[.]**”

**8. Dependent claim 8**

**(a) “The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:” (Claim 8[p])**

186. It is my opinion that the preamble to claim 8 (to the extent it is limiting) is disclosed by or obvious in light of Lambert. Thus, the preamble to claim 8 is satisfied by both Grounds 1 and 2.

187. With respect to “**a plurality of authorization records associated with a plurality of application identifiers,**” I addressed this portion of the claim in my analysis of claim 5 above, which similarly recites “the owner control information includes an authorization record and an application identifier for each of the applications.” I fully incorporate that analysis here. As discussed, Lambert discloses that policy information includes entries for applications (such as Internet Explorer and Microsoft Windows Media Player) that identify the application (such

as by file path or a hash) (“**application identifier**”) and have an associated rule (“**authorization record**”). (Lambert, [0082], [0079], [0053]-[0056], [0058]-[0063], [0068].)

188. Lambert also discloses that the plurality of authorization records and application identifiers, as policy information, are “**stored on the electronic device.**” As discussed, Lambert discloses that restriction policies are “locally maintained and/or in a group policy object distributable over a network.” (Lambert, Abstract.) For example, Lambert discloses that policy rules distributed over a network and locally maintained rules are “combined into an effective policy **502**” by a device. (*Id.*, [0064].) Accordingly, it is my opinion that Lambert discloses “**a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device.**”

(b) “**receiving requests to access the local memory from a plurality of applications operating on the electronic device;**” (Claim 8[a])

189. It is my opinion that claim 8[a] is disclosed by or would have been obvious based on Lambert. Thus, claim 8[a] is satisfied by both Grounds 1 and 2.

190. For purposes of my analysis, claim 8[a] is substantially the same as claim 1[d]. Therefore, for the reasons discussed above for claim 1[d], it is my opinion that claim 8[a] is disclosed by or would have been obvious based on

Lambert. Claim 8[a] additionally requires receiving requests from a “**plurality of applications.**” As I discussed above for claim 1[d], Lambert discloses that its system receives requests from various applications (“**a plurality of applications**”), including the applications identified in the policy rules, or the various applications in the zone of a “zone rule” or at the filepath of a “path rule.” (Lambert, [0082], [0052] (“various types of software and specific software files ... may be identified and classified”), [0063] (disclosing a “zone rule”), [0058]-[0062] (describing “path rule[s]”).) Claim 8[a] is satisfied by both Grounds 1 and 2.

(c) “**determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and:**” (Claim 8[b])

191. It is my opinion that claim 8[b] is disclosed by or would have been obvious based on Lambert. Thus, claim 8[b] is satisfied by both Grounds 1 and 2.

192. As explained above for claims 1[e] and 6, Lambert discloses determining local memory access based on policy rules, which (as discussed above for claim 8[p]) constitute “**stored authorization records and the application identifiers that are respectively associated with the plurality of applications.**” Thus, it is my opinion that claim 8[b] is disclosed by or obvious in light of Lambert.

**(d) “controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.” (Claim 8[c])**

193. It is my opinion that claim 8[c] is disclosed by or would have been obvious based on Lambert. Thus, claim 8[c] is satisfied by both Grounds 1 and 2.

194. For purposes of my analysis, claim 8[c] is substantially the same as claim 1[f]. Therefore, for the reasons discussed above for claim 1[f], it is my opinion that claim 8[c] is disclosed by or would have been obvious based on Lambert. Claim 8[c] additionally requires controlling access by a **“plurality of applications.”** As I discussed above for claim 1[f], Lambert discloses that its system controls local memory access for various applications (**“a plurality of applications”**), including the applications identified in the policy rules, or the various applications in the zone of a “zone rule” or at the filepath of a “path rule.” (Lambert, [0082], [0052] (“various types of software and specific software files ... may be identified and classified”), [0063] (disclosing a “zone rule”), [0058]-[0062] (describing “path rule[s]”).) Claim 8[c] is satisfied by both Grounds 1 and 2.

**9. Dependent claim 9**

195. For reference, claim 9 recites:

9. The method of claim 8, wherein a group containing two or more of the applications is associated with one of the authorization records.

(’571, 30:1-3 (Claim 9).)

196. It is my opinion that claim 9 is disclosed by or would have been obvious based on Lambert. Claim 9 is satisfied by both Grounds 1 and 2.

197. For example, Lambert discloses that an access restriction can be associated with a filepath, such that any applications at that filepath have the same restrictions. (Lambert, [0058]-[0062], [0082], [0068], [0066].) Lambert discloses that filepath-based access restrictions are useful since they allow certain applications—for example, “system files” necessary to be allowed to run for the computer to “work normally”—to be treated in the same way by the access restriction system. (*Id.*, [0058].) A filepath-based access restriction can therefore comprise **“a group containing two or more of the applications”**—such as a folder containing two or more applications—associated with that restriction (**“one of the authorization records”**).

198. Lambert also discloses that an access restriction can be set using a “zone rule,” wherein “the zone identifies software according to the source (e.g., the URL zone or the like) from which it is downloaded or otherwise installed.” (Lambert, [0063].) Such “zone rules” represent another way Lambert discloses **“a group containing two or more of the applications”** associated with a single restriction level (**“with one of the authorization records”**), so that “an

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

administrator can set different rules for software files classified according to their source.” (*Id.*)

199. Lambert also discloses an example access restriction policy in which multiple listings are associated with the same restriction level. (Lambert, [0082].) For example, the below excerpt shows that multiple entries are associated with the same “Disallowed” or “Unrestricted” access restriction level.

|                      |                                     |              |                |
|----------------------|-------------------------------------|--------------|----------------|
| OnlySignedLockDown   | HKCU                                | Disallowed   | CP only        |
| Path                 | %windir%                            | Unrestricted | All file types |
| Certificate          | <publisher cert>                    | Unrestricted |                |
| IexploreOnlyLockDown | HKCU                                | Disallowed   | CP only        |
| Path                 | %windir%                            | Unrestricted | All file types |
| Path                 | %programfiles%\Internet Explorer\   | Unrestricted | All file types |
| WMPOnlyLockDown      | HKCU                                | Disallowed   | CP Only        |
| Path                 | %windir%                            | Unrestricted | All file types |
| Path                 | %programfiles%\Windows Media Player | Unrestricted | All file types |
| PFNoMediaLockDown    | HKCU                                | Disallowed   | CP Only        |
| Path                 | %windir%                            | Unrestricted | All file types |
| Path                 | %programfiles%\                     | Unrestricted | All file types |
| Path                 | %programfiles%\Windows Media Player | Disallowed   | All file types |

(*Id.*) Lambert discloses that various “code authorization levels” can be defined, including “for unrestricted operation, one for end-user, one for constrained, one for

untrusted and one for revoked[.]” (*Id.*, [0079].) As shown in the example policy in Lambert, each of these “code authorization levels” can be shared by a group of applications. (*Id.*, [0082].)

**10. Independent claim 10**

**(a) “A device, comprising:” (Claim 10[p])**

200. It is my opinion that the preamble to claim 10, to the extent it is limiting, is disclosed by Lambert.

201. Lambert discloses controlling execution of applications on a computer (“**a device**”), for the same reasons explained above for claim 1[p]. For example, Figure 1 discloses a “suitable computing system environment **100** on which the invention may be implemented.” (Lambert, [0026].)

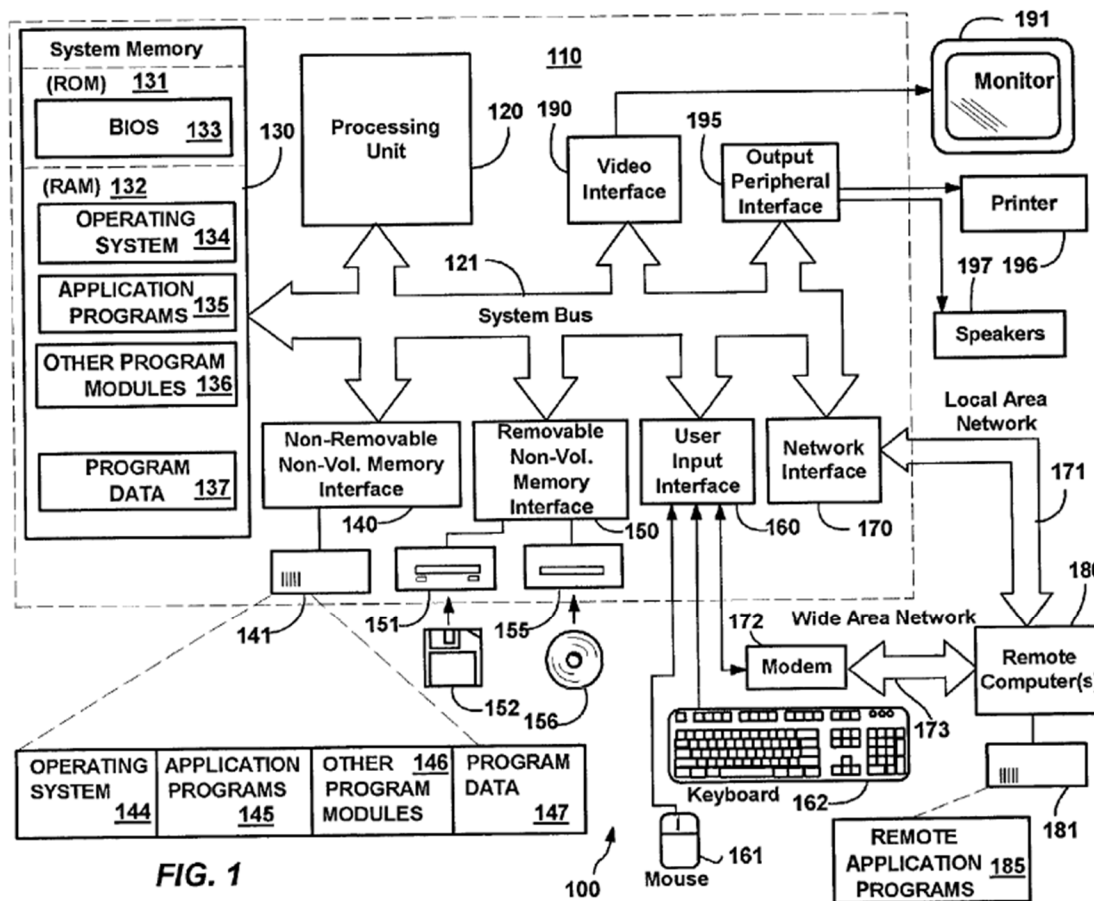


**FIG. 1**

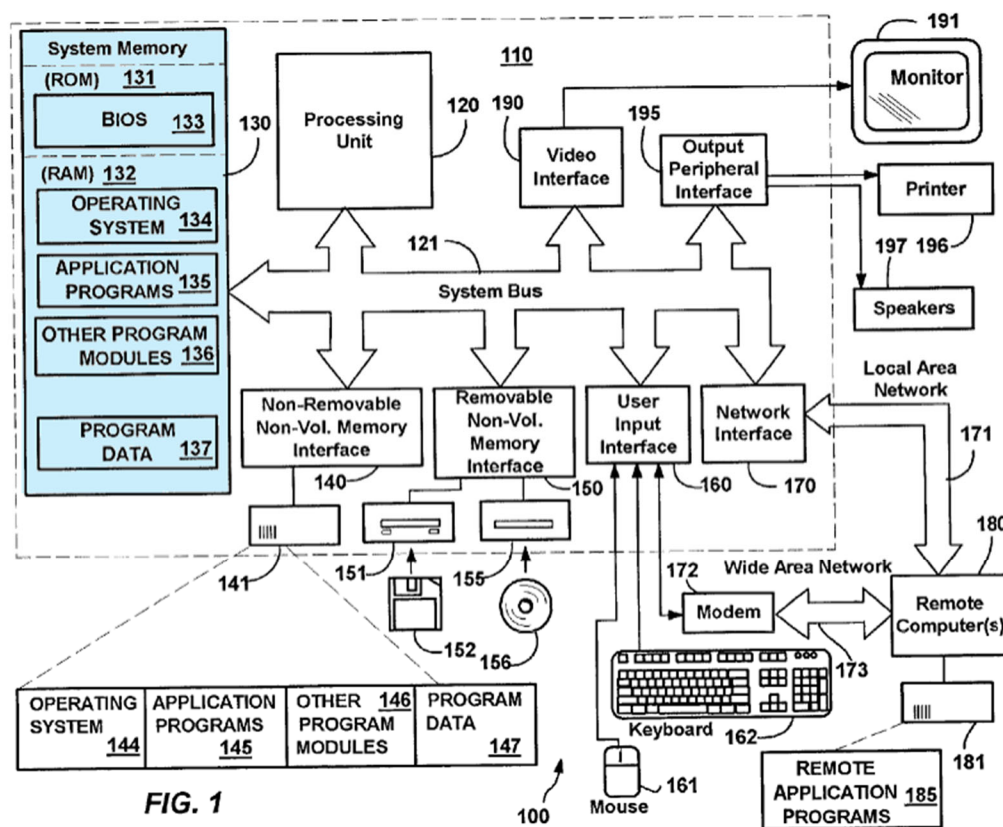
(*Id.*, Fig. 1.) Lambert's techniques are "operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the

above systems or devices, and the like.” (Id., [0027] (emphasis added).)

(b) “a memory; and” (Claim 10[a])

202. It is my opinion that claim 10[a] is disclosed by Lambert.

203. Lambert discloses that its system is implemented on a computer with a  
“memory.” For example, the “suitable computing system environment 100 on  
which the invention may be implemented” shown in Figure 1 includes a “system  
memory 130”:



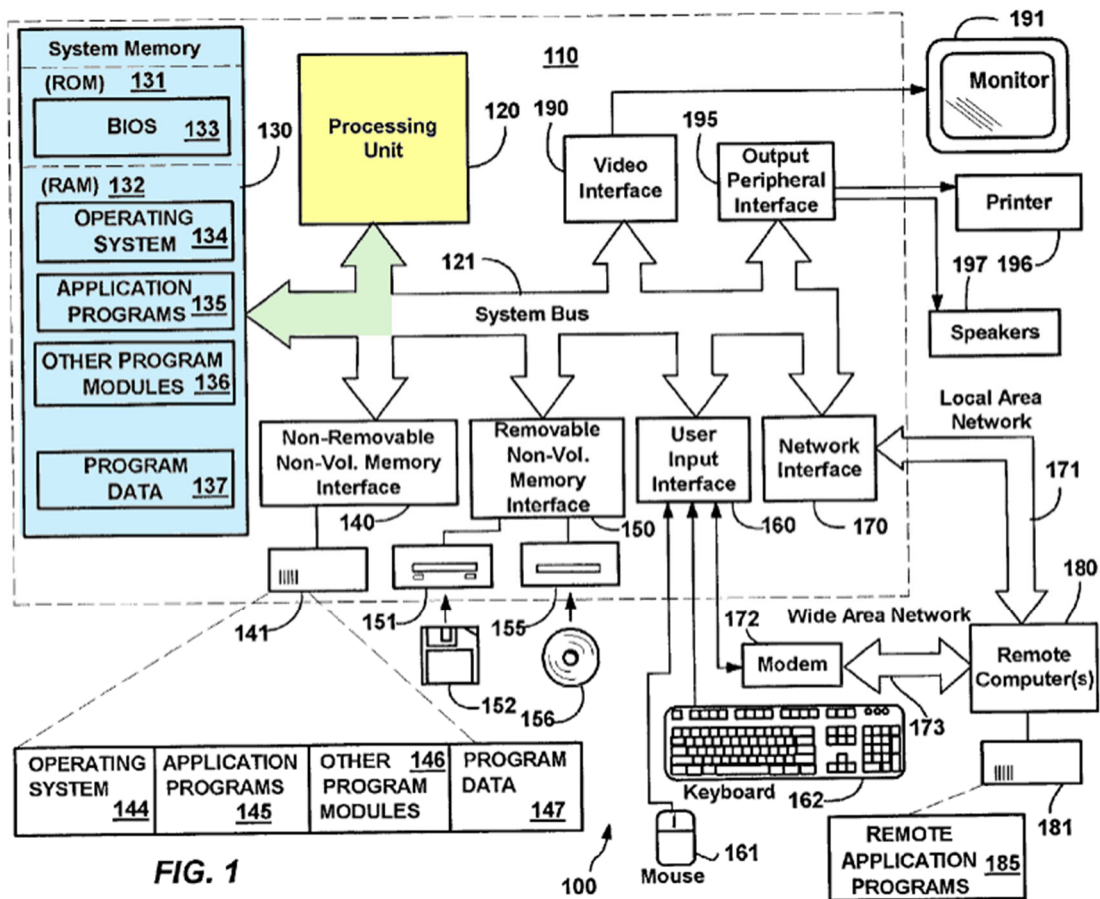
(Lambert, Fig. 1 (highlighting added).) Lambert discloses that “[t]he system  
memory 130 includes computer storage media in the form of volatile and/or

nonvolatile memory such as read only memory (ROM) **131** and random access memory (RAM) **132.**” (*Id.*, [0031].)

(c) **“a processor coupled with the memory and configured by instructions stored in the memory to:”**  
(Claim 10[b])

204. It is my opinion that claim 10[b] is disclosed by Lambert.

205. Lambert discloses that its system is implemented on a computer with a **“processor coupled with the memory.”** For example, the “suitable computing system environment **100** on which the invention may be implemented” shown in Figure 1 includes a **“processing unit 120”** coupled to the **“system memory 130”**:



(Lambert, Fig. 1 (highlighting added).) Lambert further discloses that the processor is “**configured by instructions stored in the memory**” to perform the claimed functionality. Lambert discloses that “RAM 132 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 120.” (*Id.*, [0031]; *see also id.* (disclosing that “basic input/output system 133 (BIOS), containing the basic routines that help to transfer information between elements within computer 110 ... is typically stored in ROM 131”).)

**(d) “receive owner information from an owner of the device;” (Claim 10[b][i])**

206. As discussed above for claim 1[a], it is my opinion that claim 10[b][i] is disclosed by or would have been obvious based on Lambert. In the alternative, it is my opinion that claim 10[b][i] would have been obvious over Lambert in view of Frank and/or the Windows Guidelines Book.

**(e) “receive owner control information that comprises:” (Claim 10[b][ii])**

207. As discussed above for claim 1[b], it is my opinion that claim 10[b][ii] is disclosed by or would have been obvious based on Lambert.

**(f) “a list of applications permitted for installation on the device, and” (Claim 10[b][ii][A])**

208. As discussed above for claim 1[b][i], it is my opinion that claim 10[b][ii][A] is disclosed by or would have been obvious based on Lambert. In the alternative, it is my opinion that claim 10[b][ii][A] would have been obvious over Lambert in view of Gomberg.

**(g) “permissions associated with each permitted application in the list of applications;” (Claim 10[b][ii][B])**

209. As discussed above for claim 1[b][ii], it is my opinion that claim 10[b][ii][B] is disclosed by or would have been obvious based on Lambert.

- (h) **“store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information” (Claim 10[b][iii])**

210. As discussed above for claim 1[c], it is my opinion that claim 10[b][iii] is disclosed by or would have been obvious based on Lambert, either alone or in combination with the Windows Guidelines Book.

- (i) **“receive, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 10[b][iv])**

211. As discussed above for claim 1[d], it is my opinion that claim 10[b][iv] is disclosed by or would have been obvious based on Lambert.

- (j) **“determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 10[b][v])**

212. As discussed above for claim 1[e], it is my opinion that claim 10[b][v] is disclosed by or would have been obvious based on Lambert.

- (k) **“control application access to the local memory based upon the determining.” (Claim 10[b][vi])**

213. As discussed above for claim 1[f], it is my opinion that claim 10[b][vi] is disclosed by or would have been obvious based on Lambert.

## **11. Dependent claim 11**

214. For reference, claim 11 recites:

11. The device of claim 10, wherein the request to access the local memory comprises a request to erase data from the local memory.

(’571, 30:29-31 (Claim 11).)

215. For purposes of my analysis, claim 11 is substantially the same as claim 2. Therefore, for the reasons discussed above for claim 2, it is my opinion that claim 11 is disclosed by or would have been obvious based on Lambert. Claim 11 is satisfied by both Grounds 1 and 2.

**12. Dependent claim 12**

216. For reference, claim 12 recites:

12. The device of claim 10, wherein the request to access the local memory comprises a request to read data from the local memory.

(’571, 30:32-34 (Claim 12).)

217. For purposes of my analysis, claim 12 is substantially the same as claim 3. Therefore, for the reasons discussed above for claim 3, it is my opinion that claim 12 is disclosed by or would have been obvious based on Lambert. Claim 12 is satisfied by both Grounds 1 and 2.

**13. Dependent claim 13**

218. For reference, claim 13 recites:

13. The device of claim 10, wherein the processor is further

configured to restrict modification of the owner control information after the owner control information has been stored on the electronic device.

(’571, 30:35-38 (Claim 13).)

219. Claim 13 is substantially the same as claim 4. Claim 13 additionally recites that “**the processor is further configured**” to restrict modification. In my opinion, this is not a meaningful difference. As discussed above for claim 10[b], Lambert discloses that the computing device includes a processor, and as explained for claim 10, that processor would have been “**configured**” to perform the claimed operations. A POSITA would have understood and found it obvious that the processor, in order to carry out the described policy-based controls, would further be configured to restrict modification as claimed. Claim 13 also recites restricting modification of the owner control information after it “**has been stored on the electronic device.**” As discussed above for claims 1[c] and 4, Lambert discloses storing the owner control information on the electronic device (*e.g.*, in the device’s registry), and it would have been obvious based on Lambert in view of the Windows Guidelines Book. It is therefore my opinion that claim 13 is disclosed by or obvious based on Lambert, either alone or in combination with the Windows Guidelines Book. Claim 13 is satisfied by both Grounds 1 and 2.

**14. Dependent claim 14**

220. For reference, claim 14 recites:

14. The device of claim 10, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and wherein the owner control information is provided by an external source through a wireless communication channel.

(’571, 30:39-43 (Claim 14).)

221. For purposes of my analysis, claim 14 is substantially the same as claim 5. Therefore, for the reasons discussed above for claim 5, it is my opinion that claim 14 is disclosed or obvious in light of Lambert. Claim 14 is satisfied by both Grounds 1 and 2.

**15. Dependent claim 15**

222. For reference, claim 15 recites:

15. The device of claim 14, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

(’571, 30:44-48 (Claim 15).)

223. For purposes of my analysis, claim 15 is substantially the same as claim 6. Therefore, for the reasons discussed above for claim 6, it is my opinion that

claim 15 is disclosed or obvious in light of Lambert. Claim 15 is satisfied by both Grounds 1 and 2.

**16. Dependent claim 16**

224. For reference, claim 16 recites:

16. The device of claim 10, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

(’571, 30:49-51 (Claim 16).)

225. For purposes of my analysis, claim 16 is substantially the same as claim 7. Therefore, for the reasons discussed above for claim 7, it is my opinion that claim 16 is disclosed or obvious in light of Lambert. Claim 16 is satisfied by both Grounds 1 and 2.

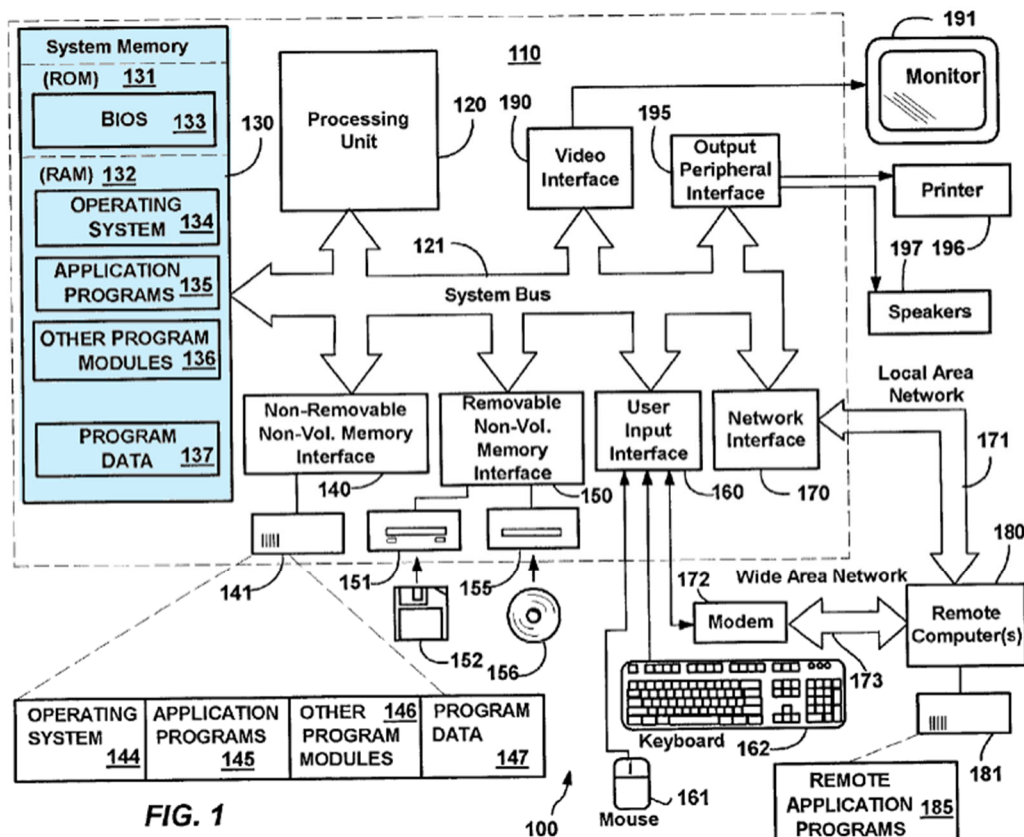
**17. Independent claim 17**

- (a) **“A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:” (Claim 17[p])**

226. It is my opinion that claim 17[p], to the extent it is limiting, is disclosed by Lambert.

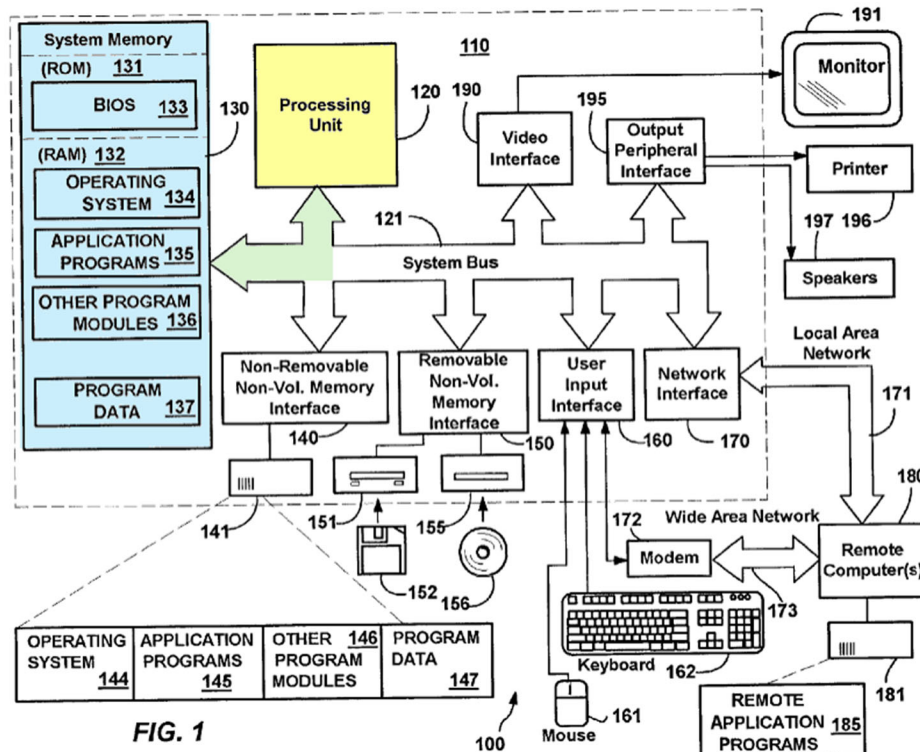
227. Lambert discloses that its system is implemented on a computer with a **“non-transitory computer-readable medium with instructions stored thereon.”**

Lambert discloses **system memory 130**, shown in Figure 1 below, which “includes computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 131 and random access memory (RAM) 132.” (Lambert, [0031] (emphasis added).)



(*Id.*, Fig. 1 (highlighting added).) Lambert further discloses that ROM 131 in system memory 130 contains “the basic routines that help to transfer information between elements within computer 110” and RAM 132 “typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 120”—*i.e.*, “**instructions.**” (*Id.*, [0031].)

228. Further, Lambert discloses “a processor”—i.e., processing unit 120:



(Lambert, Fig. 1 (highlighting added), [0031].) As discussed above in claim 10[b], Lambert discloses that processing unit 120 executes instructions stored on the system memory 130 to perform the claimed functionality. (*Id.*, [0031].)

**(b) “receiving owner information from an owner of an electronic device;” (Claim 17[a])**

229. For purposes of my analysis, claim 17[a] is substantially the same as claim 1[a]. Therefore, for the reasons discussed above for claim 1[a], it is my opinion that claim 17[a] is disclosed by or would have been obvious based on Lambert. In the alternative, it is my opinion that claim 17[a] would have been

obvious over Lambert in view of Frank and/or the Windows Guidelines Book.

**(c) “receiving owner control information that comprises:”  
(Claim 17[b])**

230. For purposes of my analysis, claim 17[b] is substantially the same as claim 1[b]. Therefore, for the reasons discussed above for claim 1[b], it is my opinion that claim 17[b] is disclosed by or would have been obvious based on Lambert.

**(d) “a list of applications permitted for installation on the  
device, and” (Claim 17[b][i])**

231. For purposes of my analysis, claim 17[b][i] is substantially the same as claim 1[b][i]. Therefore, for the reasons discussed above for claim 1[b][i], it is my opinion that claim 17[b][i] is disclosed by or would have been obvious based on Lambert. In the alternative, it is my opinion that claim 17[b][i] would have been obvious based on Lambert in light of Gomberg.

**(e) “permissions associated with each permitted  
application in the list of applications;” (Claim 17[b][ii])**

232. For purposes of my analysis, claim 17[b][ii] is substantially the same as claim 1[b][ii]. Therefore, for the reasons discussed above for claim 1[b][ii], it is my opinion that claim 17[b][ii] is obvious over Lambert.

- (f) **“storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;” (Claim 17[c])**

233. For purposes of my analysis, claim 17[c] is substantially the same as claim 1[c]. Therefore, for the reasons discussed above for claim 1[c], it is my opinion that claim 17[c] is disclosed by or would have been obvious based on Lambert, either alone or in combination with the Windows Guidelines Book.

- (g) **“receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 17[d])**

234. For purposes of my analysis, claim 17[d] is substantially the same as claim 1[d]. Therefore, for the reasons discussed above for claim 1[d], it is my opinion that claim 17[d] is disclosed by or would have been obvious based on Lambert.

- (h) **“determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 17[e])**

235. For purposes of my analysis, claim 17[e] is substantially the same as claim 1[e]. Therefore, for the reasons discussed above for claim 1[e], it is my opinion that claim 17[e] is disclosed by or would have been obvious based on Lambert.

(i) **“controlling application access to the local memory based upon the determining.” (Claim 17[f])**

236. For purposes of my analysis, claim 17[f] is substantially the same as claim 1[f]. Therefore, for the reasons discussed above for claim 1[f], it is my opinion that claim 17[f] is disclosed by or would have been obvious based on Lambert.

**18. Dependent claim 18**

237. For reference, claim 18 recites:

18. The non-transitory computer-readable medium of claim 17, wherein the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device.

(’571, 31:10-13 (Claim 18).)

238. It is my opinion that claim 18 is disclosed by or obvious in light of Lambert. Claim 18 is satisfied by both Grounds 1 and 2.

239. As discussed above for claim 1[b], Lambert discloses **“owner control information”** in the form of policy information that sets forth rules used to control how a computing device operates. As discussed for claim 5, that information includes for an application **“an authentication record”**—i.e., the associated rule (e.g., “Disallowed,” “Unrestricted,” “All file types,” and “CP only”)—and an **“identifier”**—i.e., a filepath or hash value. (Lambert, [0082], [0079], [0053], [0054], [0058]-[0063], [0068].) For example, as discussed for claim 5, Lambert

discloses an example of a policy that includes an entry for the application Internet Explorer. (*Id.*, [0082].) That entry specifies an associated path (i.e., “%programfiles%\Internet Explorer”) (“**identifier**”) and rule (i.e., “Unrestricted All File types”) (“**authentication record**”). Lambert’s policy entries for applications are consistent with the ’571 patent’s description of application authentication records. (*E.g.*, ’571, 7:46-53 (“the each application authentication records includes a field that designates the application appropriately (e.g., allowed, required, excluded, etc.) and can include a field containing an application identifier”).) Because Lambert relates to controlling application operation on a computing device, a POSITA would have understood and found it obvious for a policy to include an authentication record and an identifier “**for each application allowed to be executed on the electronic device.**” For example, Lambert explains how, with a policy, “an administrator can efficiently constrain (or prevent from running) everything on a machine, except for certain identified software files or software classifications that are allowed to run at some other security level, also set by the administrator.” (Lambert, [0011] (emphasis added).)

240. Lambert also discloses that the policy rules can include rules related to a “software publisher digital signature (e.g., certificate)” indicating the source of an application. (Lambert, [0057]; *see also id.*, [0084].) This digital signature

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

information constitutes an **“authentication record.”** (’571, 7:35-39 (“source authentication information, such as a digital signature public key associated with a digital signature private key of the owner”), 9:52-58 (“an owner control scheme in which digital signatures are used to verify data integrity and authenticate a source of data”), 10:18-21 (“authentication of a source of the signed information”), 23:21-23.)

241. Lambert discloses or renders obvious associating **“an authentication record and an identifier for each application allowed to be executed on the electronic device.”** For example, Lambert discloses that a rule could include both digital signature and identifying information. (Lambert, claim 5 (reciting “the rule that corresponds to the information only applies to a set of at least one selected file associated with the digital signature”), claim 6 (reciting “the rule that corresponds to the information applies only to files associated with the digital signature that have selected file extensions”), claim 18; *see also id.*, [0057] (“it is straightforward to have additional information be maintained in a rule and evaluated along with the signature, for example, to allow certain controls to run normally, but not others”), [0068] (“the enforcement mechanism **518** can locate a rule from the signature, path information, or zone information associated with the file **510**”), [0066].) For example, Lambert discloses that the policy rules can include “a multi-part rule that checks for allowed/restricted/disallowed signatures and

allowed/restricted/disallowed control identifiers, and taking the most restrictive result from the evaluated parts of the rule[.]” (*Id.*, [0057].) A POSITA would have been motivated to use digital signature rules for applications, since such rules can ensure that applications have a trusted source and that applications from trusted sources are not needlessly restricted. (*See, e.g., id.* (“if an enterprise digitally signs its internally developed controls, it can specify that software signed by its own publisher certificate runs normally, and also without unnecessarily prompting its users with a dialog or the like before allowing the open”), [0011].)

**19. Dependent claim 19**

242. For reference, claim 19 recites:

19. The non-transitory computer-readable medium of claim 17, wherein the request to access the local memory comprises a request to erase data from the local memory.

(’571, 31:14-16 (Claim 19).)

243. For purposes of my analysis, claim 19 is substantially the same as claim 2. Therefore, for the reasons discussed above for claim 2, it is my opinion that claim 19 is disclosed or obvious based on Lambert. Claim 19 is satisfied by both Grounds 1 and 2.

**20. Dependent claim 20**

244. For reference, claim 20 recites:

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

20. The non-transitory computer-readable medium of claim 17, wherein the request to access the local memory comprises a request to read data from the local memory.

(’571, 31:17-19 (Claim 20).)

245. For purposes of my analysis, claim 20 is substantially the same as claim 3. Therefore, for the reasons discussed above for claim 3, it is my opinion that claim 20 is disclosed or obvious based on Lambert. Claim 20 is satisfied by both Grounds 1 and 2.

**C. Summary and Overview of Hayes-Grounds Prior Art (Grounds 3-5)**

246. As noted above, this declaration addresses five grounds:

| Ground | Claims     | Basis for Challenge Under § 103                        |
|--------|------------|--------------------------------------------------------|
| 1      | 1-20       | Lambert                                                |
| 2      | 1-20       | Ground 1 + Frank, Gomberg, and Windows Guidelines Book |
| 3      | 1-8, 10-20 | Hayes in view of Sprigg                                |
| 4      | 1-8, 10-20 | Ground 3 + Frank and Guedalia                          |
| 5      | 9-20       | Ground 4 + Lambert                                     |

**1. Hayes (EX1011)**

247. **Hayes**, U.S. Patent Application Publication No. 2001/0011341 (filed May 5, 1998, published August 2, 2001) is titled “Client-Server System for Maintaining a User Desktop Consistent with Server Application User Access Permissions.” I am informed that Hayes qualifies as prior art at least because it was

filed before and published more than one year before the alleged priority date of the '571 patent.

248. Hayes describes a system for “stor[ing] access permissions for the applications for each user.” (Hayes, Abstract.) Hayes discloses an administered computer network where an administrator can control what applications each user can access on a computer terminal. Hayes discloses that “[w]hen a user attempts to log onto the system from a user station, the server receives a user log-on identifier from the user” and “build[s] a list of applications for which the user has access permission.” (*Id.*, [0013].) The user station then “uses the list to build a folder containing only the applications from the list to which the user has access permission.” (*Id.*) Further, Hayes discloses that “[f]or each user desktop preference specified by the user at an earlier time that corresponds to a user application, the access permission for the user to the user application is checked from the list, and, if the application is not included on the list, the desktop object representing the application is removed from the desktop.” (*Id.*)

249. Hayes discloses that “user applets and the desktop applet are assumed to be Java applets.” (Hayes, [0026].) Hayes further discloses that “it is understood that the invention is not limited to a Java environment” and “[t]he invention can be used in any client-server system.” (*Id.*)

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

250. Hayes discloses that an administrator can also input preferences for users and groups of users as to applications. For example, Figure 3 of Hayes shows illustrative preferences, but “[t]he terms x, y and z are intended to represent any desired preference and the values 1, 2 and 3 are arbitrary and used merely to illustrate the point.” (Hayes, [0044].)

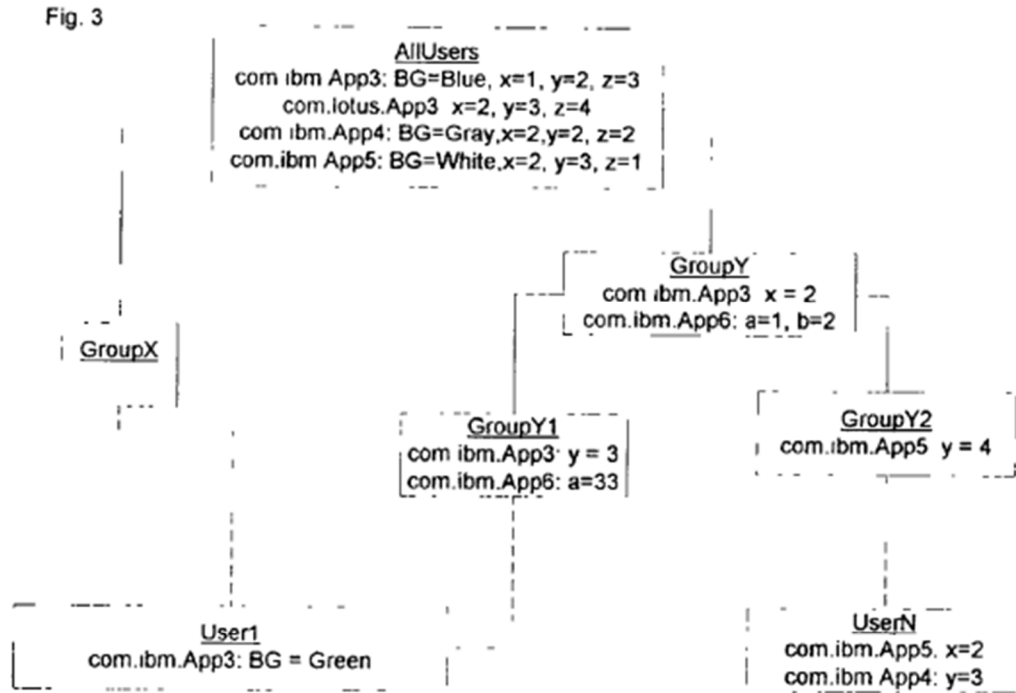


Fig. 4

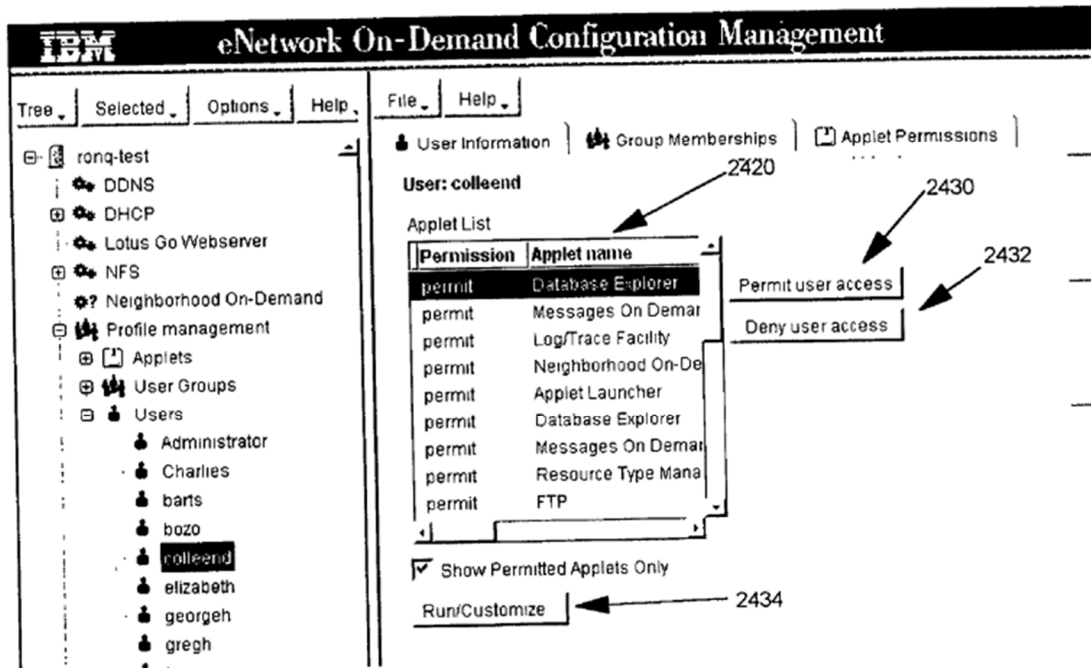
| UserList |                         |  |          |
|----------|-------------------------|--|----------|
| User     | Group                   |  | Priority |
| User1:   | AllUsers.GroupX         |  | 1        |
|          | AllUsers.GroupY.GroupY1 |  | 2        |
|          | AllUsers                |  | 3        |
| UserN    | AllUsers.GroupY.GroupY2 |  | 1        |
|          | AllUsers                |  | 2        |

(*Id.*, Fig. 3.)

251. Hayes discloses that an administrator can input user application permissions and preferences using a graphical user interface shown, for example, in

Figures 12 to 24 of Hayes. For example, Figure 24 shows an interface where the administrator can permit or deny access to applications for a user, and view applications from the point of view of a particular user based on administrative preferences. (Hayes, [0093].)

Fig. 24



(Id., Fig. 24.)

## 2. Sprigg (EX1012)

252. **Sprigg**, U.S. Patent No. 7,743,407 (filed August 13, 2002; issued June 22, 2010) is titled “Using Permissions to Allocate Device Resources to an Application.” I am informed that Sprigg qualifies as prior art because it was filed

before the alleged priority date of the '571 patent.

253. Sprigg discloses that prior art application management systems “control[] the resources of a device ... based on a user privilege level,” such that “as long as the applications were executing under those user privileges, those applications were all given the same access rights to the device.” (Sprigg, 1:53-60.) Sprigg discloses that “what is needed in the art is a system and method for protecting the resources of a device and the connected network and also increasing the flexibility of managing the device’s resources by allowing the granting rights [sic] to the resources per application.” (*Id.*, 2:11-15.) Sprigg discloses a system for restricting access to device resources on an application-by-application basis. (*Id.*, 2:23-47.) Sprigg discloses that an administrator inputs “permission lists” indicating what resources a given application can access and “associates a permission list with the application.” (*Id.*, 3:37-47.) Device resources include “memory (including primary and secondary storage), CPU time and/or access, I/O ports and particularly, the display, speakers, keyboard or keypad and a microphone.” (*Id.*, 1:37-41.) Such a system is shown in Figure 3, reproduced below:

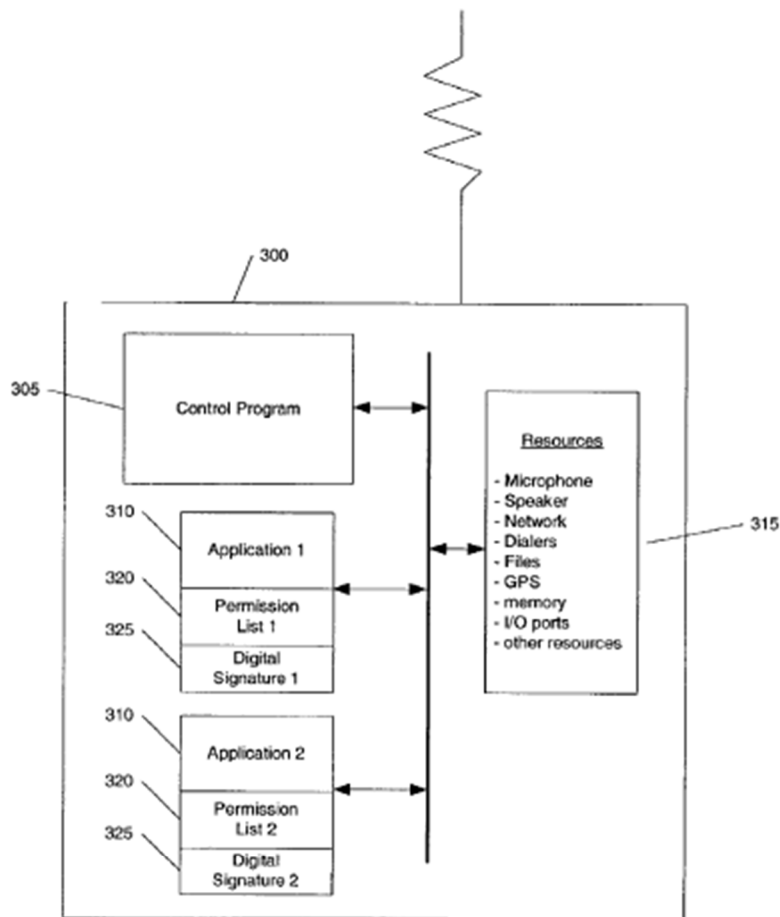


Figure 3

(*Id.*, Fig. 3.)

254. Further, Figure 4 shows a flowchart for Sprigg's system.

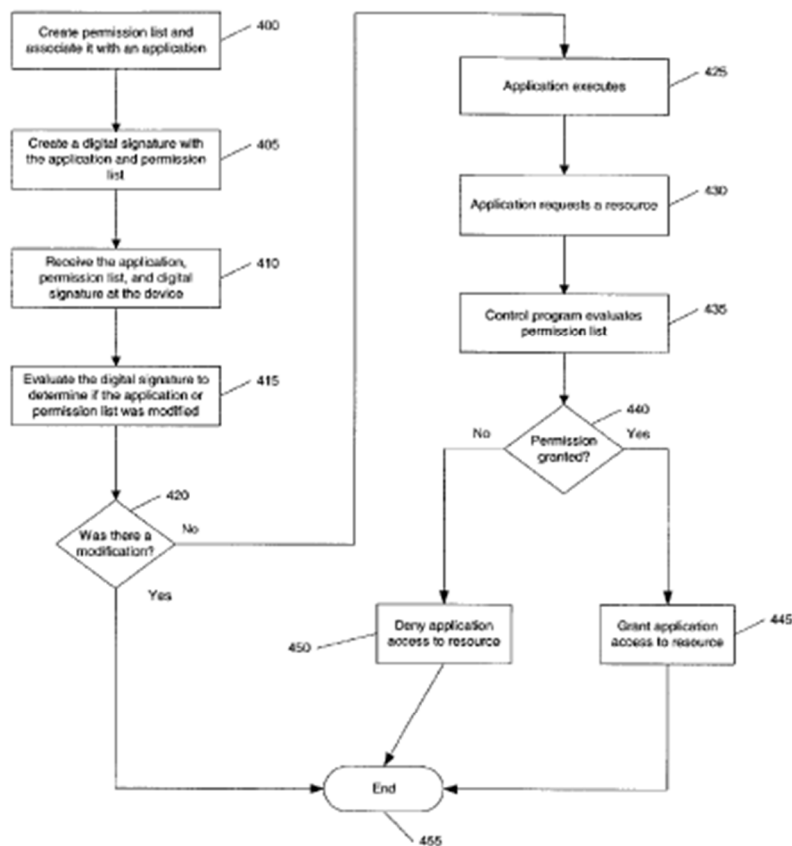


Figure 4

(Sprigg, Fig. 4.) Generally, Sprigg discloses that an application “requests a resource on the device (Step 430)”; “[t]he control program evaluates the permission list associated with the application. (Step 435)”; and the application is either allowed access to the resource or not. (*Id.*, 7:24-44.)

### 3. Frank (EX1005)

255. My summary of Frank is above for my analysis of Grounds 1-2. **Frank**,

U.S. Patent Application No. 2002/0095572 (filed January 12, 2001, published July 18, 2002), is titled “System and Method for Providing Security Profile Information to a User of a Computer System.”

#### 4. **Guedalia (EX1013)**

256. **Guedalia**, U.S. Patent No. 6,121,970 (filed November 26, 1997; issued September 19, 2000) is titled “Method and System for HTML-Driven Interactive Image Client.” I am informed that Guedalia qualifies as prior art including because it was filed before and it issued more than one year before the alleged priority date of the ’571 patent.

257. Guedalia discloses applications for providing client users with interactive image viewing software on a server-client network architecture. (Guedalia, 1:5-6.) Guedalia discloses details for how interactive applications can be provided to users on a server-client system. Guedalia discloses that “[c]lient software can take many forms, such as that of a plug-in for the browser, an Active-X control, a Java applet or a stand alone application,” where “[e]ach form has its relative advantages.” (*Id.*, 1:57-60.) For example, Guedalia discloses that plug-ins offer “a great deal of functionality, but they also require separate installation and are native to a specific platform.” (*Id.*, 1:60-63.) Guedalia discloses that “Java applets, on the other hand, automatically download from the server and install themselves,

triggered by the HTML page, and are cross-platform interoperable[.]” (*Id.*, 1:63-66.)

## **5. Lambert (EX1004)**

258. My summary of Lambert is above for my analysis of Grounds 1-2.

**Lambert**, U.S. Patent Application Publication No. 2002/0099952 (filed June 8, 2001, published July 25, 2002), is titled “Policies for Secure Software Execution.”

**D. Grounds 3-5: Claims 1-8 and 10-20 Are Obvious Over Hayes in view of Sprigg (Ground 3); Claims 1-8 and 10-20 Are Obvious Over Hayes in view of Sprigg, Frank, and Guedalia (Ground 4); Claims 9-20 Are Obvious Over Hayes in view of Sprigg, Frank, Guedalia, and Lambert (Ground 5)**

| Ground | Claims     | Basis for Challenge Under § 103 |
|--------|------------|---------------------------------|
| 3      | 1-8, 10-20 | Hayes in view of Sprigg         |
| 4      | 1-8, 10-20 | Ground 3 + Frank and Guedalia   |
| 5      | 9-20       | Ground 4 + Lambert              |

### **1. Independent Claim 1**

**(a) “A method of application control on an electronic device, the method comprising:” (Claim 1[p])**

259. It is my opinion that claim 1[p] is disclosed by Hayes.

260. Hayes discloses methods for allowing network administrators to control application use by end users. For example, Hayes discloses that network administrators can control what applications end users can download on a network. (Hayes, [0008], [0012], [0013], Figs. 8, 13, 17, 24.) Further, Hayes discloses that

network administrators can control preferences for end user applications, including how applications appear and behave to various end users. (*Id.*, [0044]-[0046], Fig.

3.) Accordingly, Hayes discloses “[a] **method of application control.**”

261. Furthermore, Hayes discloses that application control is performed on a network terminal. This could be any device on the terminal, including a device to be used by an end user. (Hayes, [0011] (disclosing that “[t]he system allows users to roam, that is, to log-in from any computer in the system at any time and have it configured automatically at run time according to the preferences stored for the user at the server”).) Hayes also provides for a “plurality of user stations, such as desktop personal computers **102**, mobile laptop computers **104**, workstations **106** (e.g., RISC computers), an administrator’s station **108** and a server **110.**” (*Id.*, [0037], Fig. 1.) Thus, Hayes discloses application control that is performed “**on an electronic device.**”

(b) “**receiving, by the electronic device, owner information from an owner of the electronic device;**” (Claim 1[a])

262. It is my opinion that claim 1[a] is disclosed by or would have been obvious based on Hayes.

263. Hayes teaches the ’571 claimed “**owner information,**” such as the ID and password information provided by the administrator disclosed in Hayes. (*E.g.*, Hayes, [0075], [0076], [0077], [0080], [0082], Figs. 7-11.) The ID and password

information in Hayes constitutes the claimed “**owner information from an owner of the electronic device**,” because much like the ’571 patent, Hayes provides that the ID and password information is input by authorized administrators of a computer network “such as a corporate intranet.” (*Id.*, [0037] (“network **100** might include wide area networking for entities such as corporations that have geographically displaced sites that are still included within the system”), [0001], [0002]-[0010] (discussing background of the invention “corporate environment,” where “a user can be connected to a corporate intranet”), [0073] (“presumably the administrator has permission to run the profile manager”).)

264. The administrators of Hayes serve to manage the activities of general “users” or “end users” of the network. (Hayes, [0039] (describing special privileges of administrators), [0036], [0004], [0025].) The information provided by these administrators is “**from an owner of the electronic device**”—*i.e.*, the owner (*e.g.*, corporation) that owns the network. (*Id.*, [0073], [0037].)

265. Much like Hayes, the ’571 patent is aimed at owner information provided by network administrators. (*E.g.*, ’571 patent, 5:63-67 (“Where the electronic device **210** is provided to a user by an employer, for example, the owner control insertion point **220** may be a computer system or device controlled by a corporate computer system administrator or IT department.” (emphasis added)),

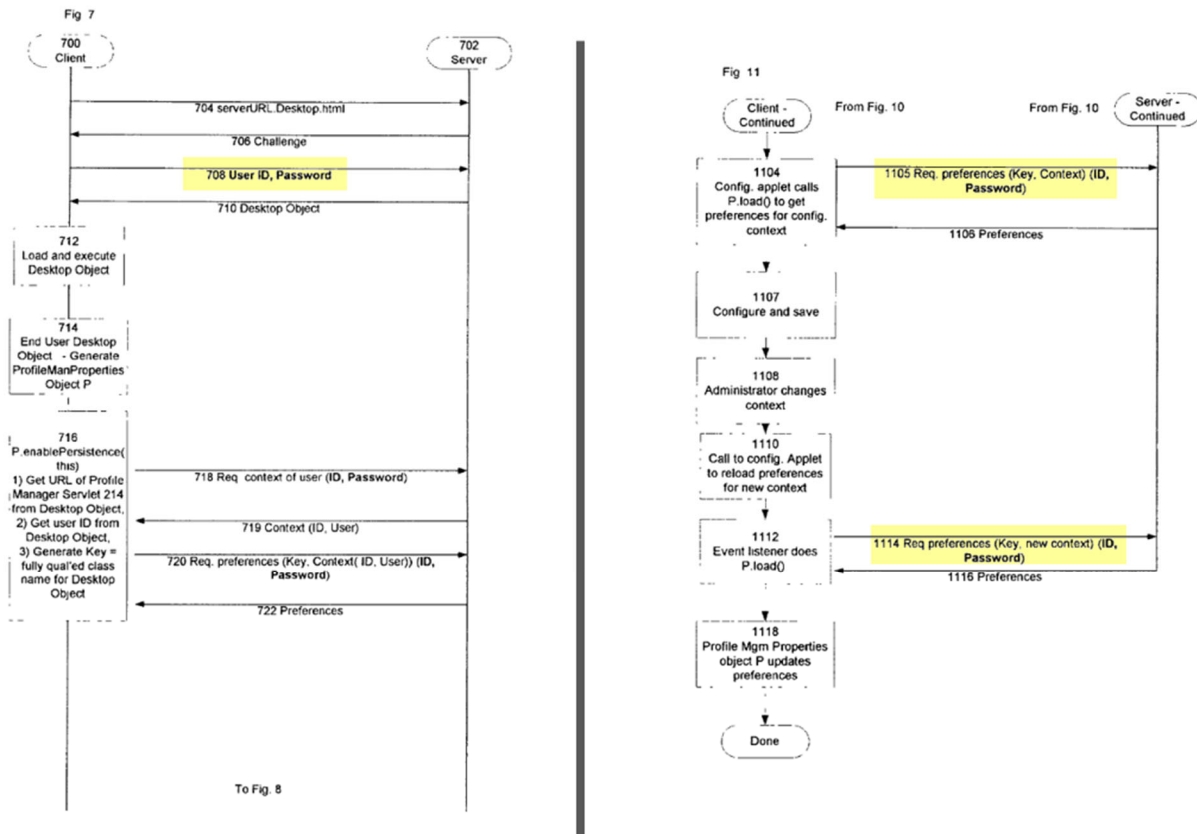
Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

6:44-50 (“In a large company, for example, corporate computer system administrators may be authorized to perform owner information insertion operations from administrator computer systems, or from any corporate computer system from which administrative functions can be accessed, thereby providing multiple owner information insertion points **220**.”) (emphasis added), 11:37-40 (“at least a first owner information insertion operation for any mobile device **30** is preferably either performed or at least authorized by an administrator”) (emphasis added), 19:14-17 (“initial owner information insertion may be performed directly by or at least under the authorization of the owner or an owner system administrator”), 9:11-17 (discussing an “owner system administrator”), 8:7-10, 10:58-62.)

266. Hayes’s ID and password information is thus “**owner information**,” consistent with the ’571 patent. (’571, 5:25-28 (“The owner information store **212** stores information, such as an owner name or other identification information[.]”) (emphasis added), 7:35-39.) Hayes’s user ID and password information constitutes the claimed “**owner information from an owner of the electronic device**.”

267. Hayes discloses that the owner information is “**receiv[ed], by the electronic device**.” Hayes discloses that the administrator user ID and password is provided on a network terminal. In Hayes, this could be any device on the terminal, including a device to be used by an end user. (*E.g.*, Hayes, [0011] (disclosing that

“[t]he system allows users to roam, that is, to log-in from any computer in the system at any time and have it configured automatically at run time according to the preferences stored for the user at the server”).) Hayes thus discloses that the owner information is “**receiv[ed], by the electronic device**” that performs the other claim limitations, as I discuss more below. Indeed, Hayes teaches that in order for an administrator to run the profile manager applet for the network, the administrator, using a client device **900**, must provide a web browser with “a user ID and password.” (*Id.*, [0073].) If the administrator “has permission to run the profile manager,” the profile manager applet is downloaded to the administrator’s terminal. (*Id.*) Further, Hayes discloses that the administrator submits a user ID and password at various steps of the process of loading and executing the profile manager applet, including step **918**, in requesting the context name of the administrator and context type; step **922**, in requesting the administrator’s preferences for the profile manager applet; step **1002**, in requesting “information about existing users, user groups, and software”; and steps **1105** and **1114** for requesting preference information for a particular context. (*Id.*, [0075], [0076], [0077], [0080], [0082], Figs. 7-11.) Three such steps in which the administrator provides user ID and password information are shown below in Hayes’s Figures 7 and 11:



(*Id.*, Figs. 7, 11 (highlighting added).) Hayes thus teaches and renders obvious the claimed “receiving, by the electronic device, owner information from an owner of the electronic device.”

268. It also would have been obvious based on Hayes that an administrator could log in to any user terminal on a network using administrative privileges. (*E.g.*, Hayes, [0011] (disclosing that “[t]he system allows users to roam, that is, to log-in from any computer in the system at any time and have it configured automatically at run time according to the preferences stored for the user at the server”), [0073].) A

POSITA would have been motivated to implement Hayes's system to allow "roam[ing]" administrators that could adjust preferences for users on the same device where those preferences would be applied or enforced. (*Id.*, [0011].) For example, Hayes discloses that an administrator in its system has the "ability to run a user application in the context of a user to set preferences for that user and application." (*Id.*, [0007].) Hayes discloses that this facilitates "administrative flexibility of operation." (*Id.*) A POSITA would have understood that allowing an administrator to log in on any user terminal or workstation would provide for further "administrative flexibility of operation" by allowing an administrator to see how the set preferences work on a particular user device.

**Obviousness Over Hayes in Light of Sprigg and Frank**

269. As I discuss below for claim 1[b][ii], allowing an administrator to input administrative credentials while using a user terminal to adjust permissions on that user terminal would have further been obvious based on Hayes in view of Sprigg and Frank.

**(c) "receiving, by the electronic device, owner control information that comprises:" (Claim 1[b]) and "a list of applications permitted for installation on the electronic device, and" (Claim 1[b][i])**

270. It is my opinion that claim 1[b] and claim 1[b][i] are both disclosed by or would have been obvious based on Hayes.

271. The list of allowed applications disclosed by Hayes is “**owner control information**,” because it controls what applications an end user can download on his or her terminal. As discussed above, such information is “**owner...information**,” because it is provided by an administrator authorized by a network owner (*e.g.*, the associated corporation). (Hayes, [0037], [0001], [0002]-[0010], [0073].) Considering this information “**owner...information**” is consistent with the ’571 patent’s administrator-provided “owner” information and “owner” control information. (’571, 5:63-67, 6:44-50, 11:37-40, 19:14-17, 9:11-17, 8:7-10, 10:58-62.) As explained above, Hayes teaches “**receiving, by the electronic device, owner control information[.]**”

272. Hayes discloses receiving “**a list of applications permitted for installation on the electronic device**” set by the administrator of a computer network—for example, of a corporate intranet system.

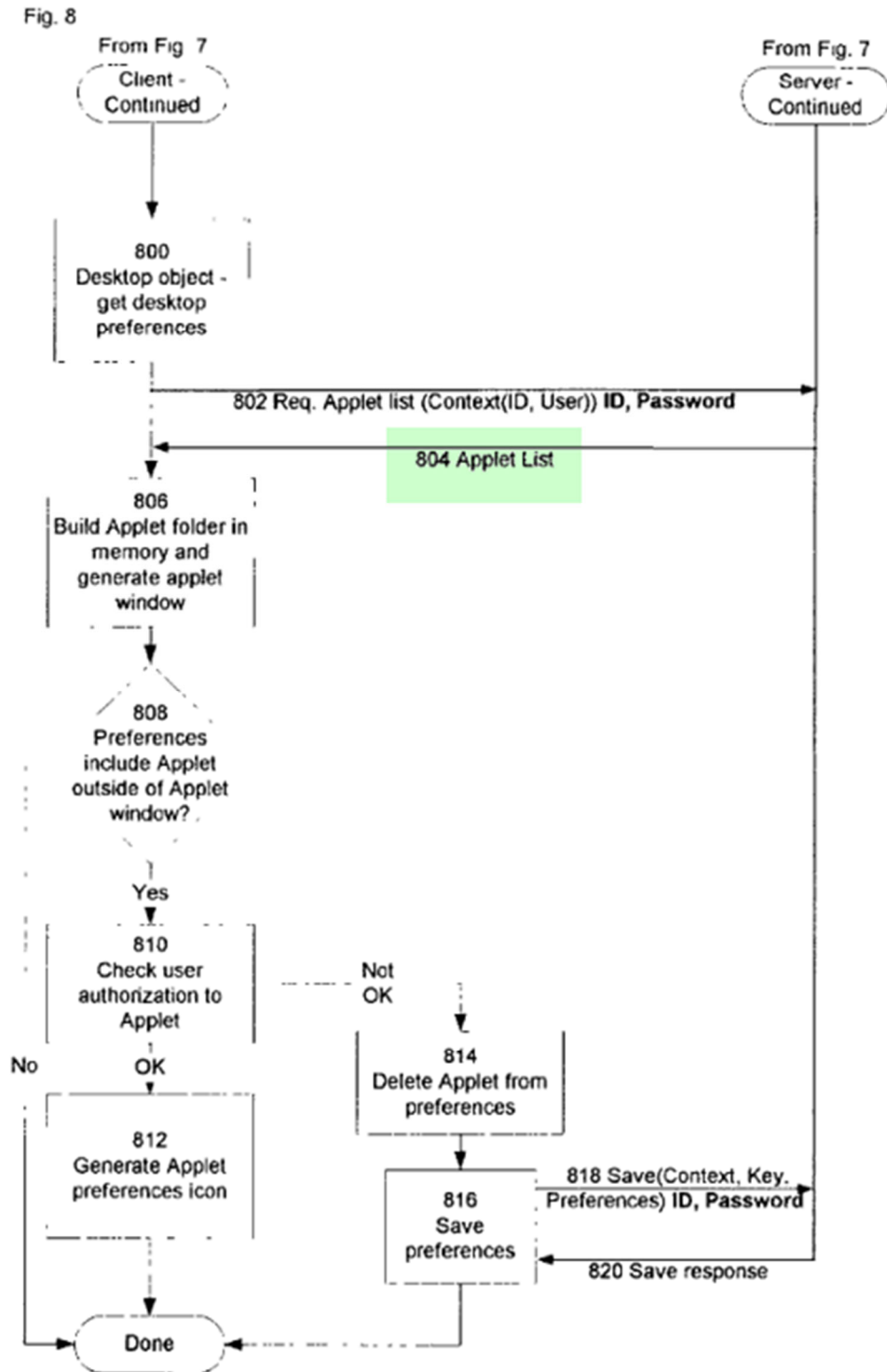
273. Hayes teaches that when an end user brings up the desktop on a terminal, the “desktop objects calls a method ... to get a list of the software to which the user has access permission.” (Hayes, [0071] (emphasis added).)

274. Hayes discloses that the server provides “a user friendly name, the applet’s URL, the URL of an icon for the applet, etc. (information that is required for the desktop to represent the applet on the desktop and to load and launch it).”

(Hayes, [0071] (emphasis added).)

275. Moreover, “the server stores a plurality of user applications for downloading to user stations and further stores access permissions for the applications.” (Hayes, [0013]) (emphasis added).) Hayes explains that the server uses a user’s identifying information to “build a list of applications for which the user has access permission.” (*Id.*) The server further “downloads to the station a list of applications to which the user has access permission,” and “[t]he user station uses the list to build a folder containing only the applications from the list to which the user has access permission.” (*Id.*; *see also id.*, claim 1 (reciting “downloading to the station the list of applications for which the user has access permissions” and requesting “a download of the corresponding application to the user station”), [0012].)

276. The computer terminal’s receipt of the list of allowed software from the server (shown **highlighted** below in Hayes’s Figure 8) thus constitutes receiving **“a list of applications permitted for installation on the electronic device.”**

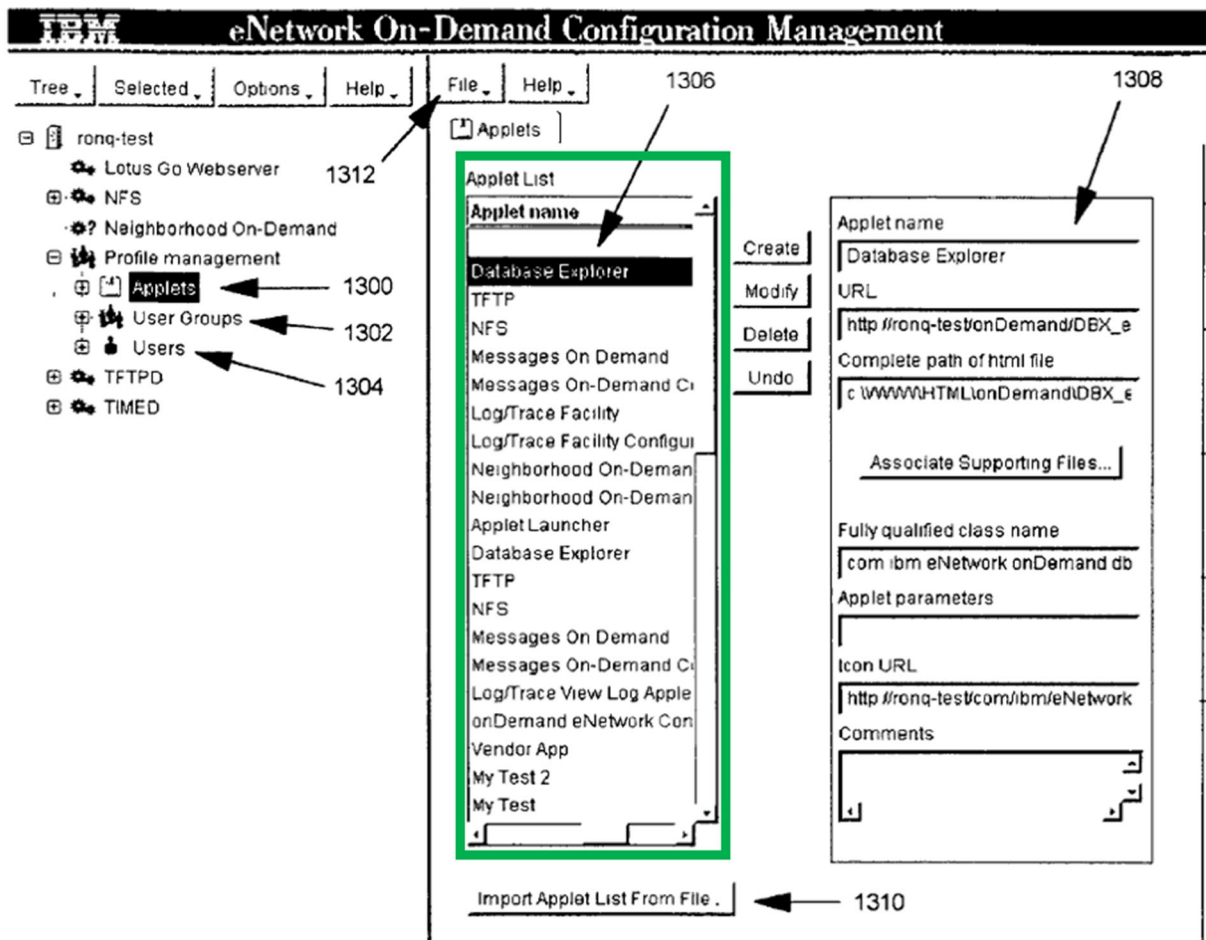


(Hayes, Fig. 8 (highlighting added), [0025] (“Applet” refers to an independent

software module that runs within a Java enabled web browser.”.) As explained above, Hayes’s list of applications permitted for installation is received on the electronic device.

277. Hayes further discloses screenshots of an interface where an interface can set the list of allowed software applications for a network. For example, in Figure 13, Hayes shows an “Applet List” with options for an administrator to “Create” or “Delete” applets:

Fig. 13



(Hayes, Fig. 13 (highlighting added), [0085].) Further, Hayes discloses a screenshot of an interface where an administrator can allow a subset of permitted applications for a particular user (Figure 24), or for groups of users (Figure 17):

Fig. 24

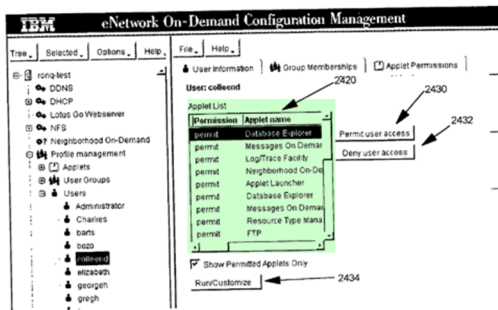
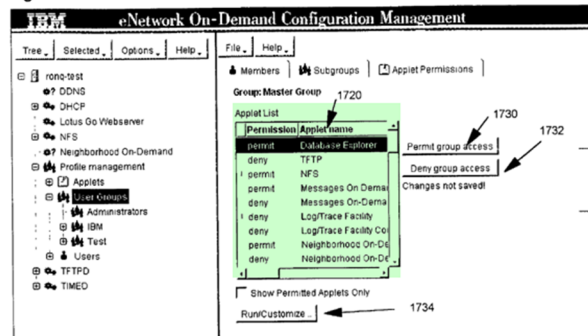


Fig. 17



(*Id.*, Figs. 24 & 17 (highlighting added), [0093], [0088].) This is thus an example of “owner control information” that comprises a “list of applications permitted for installation on the electronic device.”

278. I understand that in the parallel district court litigation, Petitioner proposed that the term “a list of applications permitted for installation” should be construed as “a list of applications permitted by the owner for installation.” Patent Owner proposes no construction needed. In my opinion, Hayes discloses claim 1[b][i] under Petitioner’s proposed construction of this term. As I discussed above, Hayes discloses that the list of allowed applications is provided by an administrator, including in a corporate context where such an administrator is acting on behalf of the owner (*e.g.*, the corporation). The allowed applications are

“permitted by the owner,” since they are permitted by the administrator.

279. I understand that Patent Owner in the parallel district court litigation has argued “no construction” is needed, because the claimed “list of applications permitted for installation on the electronic device” can be any “list of applications permitted for installation on the electronic device.” In my opinion, Hayes discloses claim 1[b][i] under Patent Owner’s position for the term (or any reasonable construction), for the same reasons identified above.

**Obviousness Over Hayes in View of Guedalia**

280. As I discussed above, Hayes discloses or renders obvious claim 1[b][i]. The **Guedalia** (EX1013) reference provides further support that Hayes discloses or renders obvious claim 1[b][i]. Claim 1[b][i] would have further been obvious to a POSITA over Hayes in view of **Guedalia**.

281. Guedalia discloses software for providing interactive applications on a client device in a server-client computer network system. (Guedalia, 1:5-17.) Guedalia discloses that such software “can take many forms, such as that of a plug-in for the browser, an Active-X control, a Java applet or a stand alone application.” (*Id.*, 1:57-59.) Guedalia discloses that “[e]ach form has its relative advantages.” (*Id.*, 1:59-60.) For example, Guedalia discloses that plug-ins offer “a great deal of functionality, but they also require separate installation and are native to a specific

platform.” (*Id.*, 1:60-63.) Guedalia discloses that “Java applets, on the other hand, automatically download from the server and install themselves, triggered by the HTML page, and are cross-platform interoperable[.]” (*Id.*, 1:63-66 (emphasis added).)

282. As discussed above, Hayes discloses that its system can be used with Java applets, where the applets constitute the applications in the “**list of applications permitted for installation.**” (Hayes, [0011] (“in the preferred embodiment, user applets and the desktop applet are assumed to be Java applets”), [0025] (“‘Applet’ refers to an independent software module that runs within a Java enabled web browser.”); *id.*, Fig. 8; *see also id.* [0026], [0013], [0012].)

283. Guedalia supports that Hayes discloses or renders obvious a “**list of applications permitted for installation.**” Guedalia indicates that a POSITA would have understood that Hayes’s Java applets are installed on a user terminal in Hayes’s system. (Guedalia, 1:63-66.) A POSITA would have understood (or it would have been obvious to a POSITA) that Hayes’s Java applets are both downloaded and installed on a user computer.

284. Further, it would have been obvious based on Hayes in light of Guedalia that the user computers in Hayes would “receiv[e] ... **a list of applications permitted for installation on the electronic device.**” In the combination of Hayes

and Guedalia, a user computer would receive a list of Java applets, which would be both downloaded and installed on a user computer.

285. **Motivation to Combine**: Hayes and Guedalia are analogous art in a similar field. For example, both references relate to providing applications in a server-client computer network architecture. (Hayes, [0001] (“the invention relates to server-based storage of software preferences (configuration data) for software retrieved from a server and executing at the desktop computer”), [0002]; Guedalia, 1:5-6 (“The present invention relates to the interactive viewing of images over the Internet.”), 1:57-2:3, 2:40-54.) Further, as discussed above, both references use Java applets. (Hayes, [0011], [0025], Fig. 8; *see also id.* [0026], [0013], [0012]; Guedalia, 1:57-2:3, 5:18-20, 12:21-30, 13:8-17.)

286. A POSITA would have been motivated to combine Hayes and Guedalia in determining how to implement Hayes’s system. As Hayes and Guedalia indicate, there are various types of software on which applications can be provided in a server-client computer network architecture. (Hayes, [0026] (“The invention can be used in any client-server system ... to use proprietary communication protocols and applications written and compiled in any desired programming language.”); Guedalia, 1:57-2:3 (“Client software can take many forms[.]”).) Accordingly, in implementing Hayes’s system, a POSITA would have been motivated to look to

Guedalia, since Guedalia discusses the use of various types of software to provide applications in a client-server architecture and the relative advantages of the various types. (See, e.g., Guedalia, 1:57-2:3.) A POSITA would have looked to Guedalia for insight into what types of software (e.g., plug-ins, Java applets, or a stand alone application) would have been suited for a particular implementation of Hayes's system.

287. Further, a POSITA would have been motivated to look to Guedalia for implementation details on Java applets. Guedalia discusses differences in how various types of server-client applications operate. For example, as discussed above, Guedalia discloses that plug-ins must be separately installed after being downloaded, whereas "Java applets, on the other hand, automatically download from the server and install themselves." (Guedalia, 1:60-67.) A POSITA would have looked to Guedalia to better understand the user experience for Java applets—e.g., what steps a user in Hayes's system would need to go through in order to use Java applets in the Hayes system.

288. A POSITA would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques without undue experimentation. The Hayes and Guedalia combination is standard computing technology. For example, Java applets were

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

introduced in 1995—around seven years prior to the 2002 alleged ’571 patent priority date. (EX1014 (S. Rajesh Kumar *et al*, “A Study on Ajax in Web Applications with Latest Trends” (2013)), p.002 (“Java applets were introduced in the first version of the Java language in 1995.”).) The proposed combination would have involved nothing more than the routine implementation of known techniques.

289. Guedalia, like Hayes, is analogous art to the ’571 patent. Guedalia is similarly related to offering applications to a user in a managed network. (*E.g.*, Hayes, [0006] (“However, flat systems are inflexible in many environments, especially in environments having large numbers of users. It is desirable to provide an administrative tool supporting the organization of preference information into a hierarchical structure.”), [0005] (“[I]n a worse case, the user’s computer may crash.”); Guedalia, 1:5-17; ’571, 1:41-43, 6:44-50, 1:67-2:4 (“However, this type of scheme is sometimes circumvented by a user by either deleting the owner policy file or replacing the owner policy file with a user policy file which may include fewer restrictions than the owner policy file.”).)

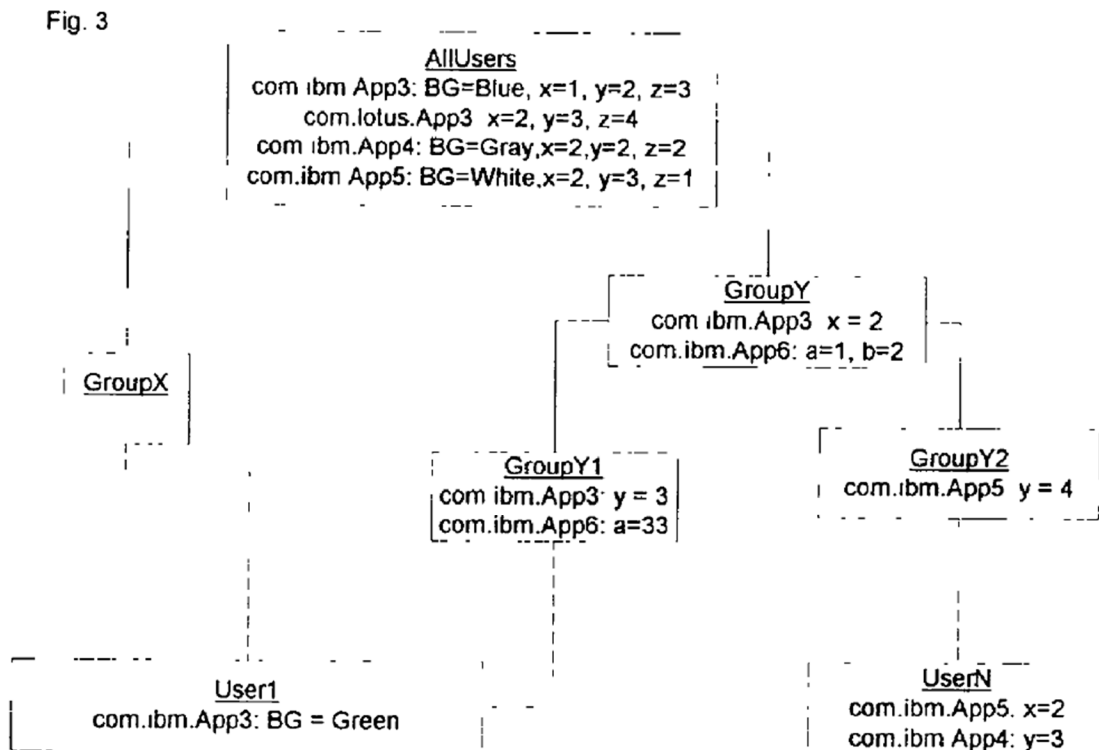
**(d) “permissions associated with each permitted application in the list of applications;” (Claim 1[b][ii])**

290. Claim 1[b][ii] is obvious over Hayes in light of **Sprigg** (EX1012; U.S. Patent No. 7,743,407).

291. Hayes discloses that an administrator can provide “preferences” for

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

each allowed application in its system. For example, Hayes discloses that an administrator can input various preferences for specific users and groups of users, which cause differences in application behavior or appearance. (Hayes, [0044]-[0046] (discussing “default background,” “screen font for the desktop,” and “default font”).) In Figure 3 (reproduced below), Hayes discloses various application preferences represented by terms x, y, and z and values 1, 2, and 3. (*Id.*) Hayes discloses that “[t]he terms x, y and z are intended to represent any desired preference and the values 1, 2 and 3 are arbitrary and used merely to illustrate the point.” (*Id.*, [0044].)



(*Id.*, Fig. 3.)

292. Hayes does not explicitly disclose an administrator using its system for providing “**permissions**” for the allowed applications on the network. However, it would have been obvious to provide application “**permissions**” for allowed applications on Hayes’s system in light of Sprigg (EX1012; U.S. Patent No. 7,743,407).

293. Sprigg discloses a computer network where a wireless device **300** contains “applications **310** each with a permission list **320**.” (Sprigg, 5:41-43.) Sprigg discloses that “each application [**310**]<sup>4</sup> may have a separate permission list associated with that application[.]” (*Id.*, 5:45-48.) Sprigg further discloses that these permissions associated with each application “contain[] a listing of the resources **315** and an indication whether the application has permission to access any of the specific resources **315** on the device.” (*Id.*, 5:63-66.) For example, Sprigg discloses that the permission lists can control access to “memory, including primary and secondary

---

<sup>4</sup> The specification in Sprigg indicates “application **110**.” (Sprigg, 5:45.) However, a POSITA would have understood that this is a typo and should refer to “application [**310**],” consistent with the numbering of Figure 3 and the surrounding discussion in the specification. (*Id.*, Fig. 3, 5:39-53.)

storage” and “files stored in memory, including the read, write and modify operations on such files.” (*Id.*, 4:14-21.) The permission lists can further be “created by an intermediate authority,” including “determination of the application’s access to the device’s resources by those authorities, entities, or parties that may be affected by the misuse of a device’s resource.” (*Id.*, 6:12-17.)

294. **Motivation to Combine:** It would have been obvious to a POSITA to implement Sprigg’s permission lists in the network control system disclosed by Hayes. In such a system, in addition to providing a list of allowed applications and preferences for those applications like Hayes discloses, an administrator would further provide a permission list for each allowed application indicating whether the application has permission to access resources on the device, including memory.

295. In the combination between Hayes and Sprigg, an administrator would provide “**permissions associated with each permitted application in the list of applications.**” For each allowed application on Hayes’s network, an administrator could input a set of permissions for that application—for example, on a user group or per-user basis. This could be implemented, for example, via an additional screen on the administrator profile manager application shown in Hayes’s Figures 12 to 24.

296. Hayes and Sprigg are analogous art in a similar field. For example, both references relate to networked computer systems managed by administrators.

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

(Hayes, [0001] (“the invention relates to server-based storage of software preferences (configuration data) for software retrieved from a server and executing at the desktop computer”); Sprigg, 1:13-15 (“The present invention relates to ... the granting of device resources per application.”), 1:31-36 (“Security concerns on the wireless device include controlling the environment the best way possible so that an application cannot, intentionally or unintentionally, degrade or corrupt other files on the wireless device or the network on which the wireless device communicates.”), 3:36-41 (indicating that “system administrator ... may create or provide input to creating this permission list for the application when used on the device”).) Further, Hayes and Sprigg both relate to management of applications. (Hayes, [0001] (invention “relates to the new and evolving field of network computing, in which desktop computer users use a personal computer ... to gain access to applications which are then executed on the desktop computer”); Sprigg, 1:13-15 (“The present invention relates to processing of applications for use in a computer device, and more particularly, to the granting of device resources per application.”).)

297. A POSITA would have been motivated to combine Hayes with Sprigg to allow for more fine-grained management of application use. Hayes’s system determines whether or not applications are available to a user at all—*e.g.*, for installation on a device. (Hayes, [0013] (disclosing system that “downloads to the

station a list of applications to which the user has access permission,” and “[t]he user station uses the list to build a folder containing only the applications from the list to which the user has access permission”).) Sprigg’s system determines what specific operations applications are allowed to do—*e.g.*, what resources applications can access. (Sprigg, 5:63-66, 4:14-21, 6:12-17.) A POSITA would have understood that incorporating Sprigg’s application permissions into Hayes’s system would be advantageous. For example, Sprigg discloses that its application-specific restrictions facilitate “increasing the flexibility of managing the device’s resources by allowing the granting rights to the resources per application.” (*Id.*, 2:11-15.) Sprigg indicates that such application-specific restrictions are an improvement over prior art systems, which only conferred access or denied access to entire applications depending on a user’s privileges. (*Id.*, 1:61-2:10.) A POSITA would have recognized that Sprigg’s discussion of prior art systems is similar to the system Hayes discloses, since both Hayes and the prior art systems Sprigg describes manage whether or not users can access entire applications. Accordingly, a POSITA would have been motivated to incorporate the improvements of Sprigg into Hayes’s system.

298. A POSITA would have been motivated to implement Sprigg’s permission lists on Hayes’s system to improve computer security. For example, Sprigg discloses that “[i]t is desirable control [sic] the application’s access to the

device resources as a security measure to limit any damage an application may have on the device, or other devices connected to the device.” (Sprigg, 1:45-48.) Sprigg discloses that the damage from an application without resource access restrictions may be “intended via a virus on the application or may be unintended where the application executes with poorly written code that unintentionally dominates a resource and makes it unavailable or damaged to other applications.” (*Id.*, 1:48-52.) Sprigg’s solution to “overcome the shortcomings of existing systems” is “allowing an application access to a device’s resources based on a set of permissions associated with the application”—*i.e.*, permission lists. (*Id.*, 2:19-22.) Such disclosures would have motivated a POSITA to improve the security of Hayes’s system by allowing an administrator to provide permission lists for allowed applications.

299. A POSITA would have been further motivated to combine Hayes and Sprigg based on Hayes’s disclosures regarding administrators setting preferences for user applications. For example, as discussed above, Hayes discloses that an administrator can input various preferences for specific users and groups of users, which cause differences in application behavior or appearance. (Hayes, [0044]-[0046] (discussing “default background,” “screen font for the desktop,” and “default font”).) A POSITA would have recognized these administrator-provided application preferences to be similar to Sprigg’s disclosure of application-specific permissions.

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

300. In my opinion, a POSITA would have had more than a reasonable expectation of success and could have implemented the combination of Hayes and Sprigg using conventional techniques without undue experimentation. It is my opinion that the proposed combination would have involved nothing more than the routine implementation of prior art devices according to known techniques. For example, the '571 patent specification recognizes that a “known scheme for controlling operation of electronic devices” was for an “an owner [to] load[] a policy file onto a device to restrict the type of operations or software applications that may be executed by the device.” ('571, 1:63-67.)

301. Hayes and Sprigg are both analogous references to the '571 patent. They are generally related to computer systems and management of applications by administrators. (Hayes, [0001] (“the invention relates to server-based storage of software preferences (configuration data) for software retrieved from a server and executing at the desktop computer”); Sprigg, 1:13-15 (“The present invention relates to ... the granting of device resources per application.”), 3:36-41; '571, 1:41-43 (“This system relates generally to electronic devices, and in particular to controlling application installation of such devices by a device owner.”).) Both Hayes and Sprigg relate to computer security and administration across multiple users. (Hayes, [0005] (“[I]n a worse case, the user’s computer may crash.”), [0006] (“However, flat

systems are inflexible in many environments, especially in environments having large numbers of users. It is desirable to provide an administrative tool supporting the organization of preference information into a hierarchical structure.”); Sprigg, 1:31-36 (“Security concerns on the wireless device include controlling the environment the best way possible so that an application cannot, intentionally or unintentionally, degrade or corrupt other files on the wireless device or the network on which the wireless device communicates.”); ’571, 1:67-2:4 (“However, this type of scheme is sometimes circumvented by a user by either deleting the owner policy file or replacing the owner policy file with a user policy file which may include fewer restrictions than the owner policy file.”).)

**Obviousness Over Hayes in Light of Sprigg and Frank**

302. As discussed above, claim 1[b][ii] would have been obvious based on Hayes in light of Sprigg. Claim 1[b][ii] would have further been obvious based on Hayes in light of Sprigg and **Frank** (EX1005; U.S. Patent Application No. 2002/0095572).

303. Much like Hayes and Sprigg, Frank discloses a computer security system managed by administrators to control the activity of end users. (Frank, [0002] (“The present invention generally relates to computer resource security[.]”), [0029] (user of security application is “a system administrator (i.e., a user authorized

to set and/or change the security profile of the system **12**)”), [0005]-[0012] (discussing system administrators as “Related Art”).) Frank discloses a security application that an administrator can access on the device for which the administrator is setting security policy—applying the security rules input by the administrator in real time. (*Id.*, [0043] (“In response, the security application **52** modifies the machine state of the computer system **50** such that the security rules selected by the system administrator are enforced by the computer system **50** (e.g., by operating system **16**) during any subsequent operation until the security profile is later changed.”); *id.*, [0040]-[0042], [0028]-[0030] (“In other words, the security application **13** includes data that defines a list of security rules for locking down the computer system **12**.”).) This allows the administrator to see the impact of changing a security policy on the target device immediately, allowing the user to easily see the consequences of the policy in case there are undesirable results and modify the policy accordingly. (*Id.*, [0011] (administrator “may mistakenly add undesirable rules and/or remove desirable rules”), [0012] (in the prior art, “[a]ttempting to discover and remedy the undesirable effects introduced by the system administrator in changing the security profile can be difficult and/or time consuming”).)

304. It would have been obvious in light of Frank to implement the

combined system of Hayes and Sprigg to enable the administrator to log in to a user terminal using administrative credentials (“**owner information**”) and adjust the “**owner control information**” for that computer (allowed applications and application resource restrictions)—all on the user computer terminal where that “**owner control information**” would subsequently be enforced for a non-administrative user. Per Frank’s disclosures, this combination would allow an administrator to view the impact of any security policy setting (*e.g.*, application permissions) in real time on the device where that policy is to be enforced.

305. **Motivation to Combine**: Hayes, Sprigg, and Frank are analogous art in a similar field. For example, each reference relates to administrators setting computer security policy for end users. (Frank, [0002] (“The present invention generally relates to computer resource security[.]”), [0029] (user of security application is “a system administrator (i.e., a user authorized to set and/or change the security profile of the system 12)”), [0008] (“Normally, a security application only allows the system administrator or a user designated by the system administrator to change the computer system's security profile.”), [0005]-[0007], [0009]-[0012]; Hayes, [0002] (describing advantages of having “a small number of server administration experts, rather than having many users struggle with the problems of software installation, upgrades and computer administration”), [0010]

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

(disclosing disadvantages of prior art that is “time consuming and inconvenient for an administrator”), [0027], [0001], [0004]; Sprigg, 3:37-41 (“The developer of the application, system administrator, or other authority, such as a carrier or device manufacturer, may create or provide input to creating this permission list for the application when used on the device.”).)

306. A POSITA would have been motivated to implement a security application on a user terminal on the combined Hayes-Sprigg system to enable an administrator to easily see the results of changes to security policy. A POSITA would have understood this as advantageous, including based on disclosures in Hayes. Hayes discloses that one of the advantages of its system over the prior art is that it allows an administrator to adjust end user preferences for applications and then view the applications from the perspective of a particular user. (Hayes, [0088] (“an administrator can select an applet from **1720** and click the ‘Run/Customize’ button **1734** to execute the user applet under the selected context”), [0007] (“The prior art does not allow this administrative flexibility of operation. In other words, in the prior art, to the best of our knowledge, an administrator does not have the ability to run a user application in the context of a user to set preferences for that user and application.”), [0093], [0094], Figs. 17, 24.) A POSITA would have viewed allowing an administrator to log into a user terminal to view security policies from

a user's perspective to be a further extension of the "flexibility of operation" Hayes encourages for administrator settings. (*Id.*, [0007].)

307. A POSITA would have further been motivated to combine Hayes, Sprigg, and Frank to streamline the process of inputting security policy for a computer. A POSITA would have understood that if an administrator could easily see the results of a security policy in real time on a user terminal, this would make it less likely that the security policy would need to go through multiple (potentially time-consuming, costly) iterations. Instead, an administrator could simply adjust the security policy, see the results, and adjust the policy further if necessary—cutting out potentially costly time for a policy to be rolled out to an entire organization and cause issues before being revised. Hayes discloses that it is advantageous to streamline the user experience for an administrator—disclosing, for instance, that an advantage of its system over prior art systems is that prior art systems required "relaunching software each time a context is changed," which was "time consuming and inconvenient for an administrator." (Hayes, [0010].) A POSITA would have understood that streamlining the security policy input process would have decreased the time and improved the convenience associated with an administrator's inputting of security policy.

308. A POSITA would have been particularly motivated to combine Frank

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

with Hayes in combination with Sprigg. Sprigg discloses restricting application resource access. A POSITA would have understood that it is particularly important for an administrator to view how an application resource access security policy is implemented on a user device, because such policies can have “undesirable effects” if implemented poorly or in error. (Frank, [0012]; *see also id.*, [0011].) For example, Frank discloses that “it is possible that the errors introduced by changing the security profile lock authorized users and even the system administrator out of the computer system and/or the security application, thereby making the process of correcting for the administrator’s mistakes even more difficult and problematic.” (*Id.*, [0012]; *see also id.*, [0011] (discussing “human error” and “administrator’s lack of understanding the ramifications of the changes” to a security policy).) Similarly, Sprigg indicates that an underinclusive policy that does not put adequate restrictions on applications can lead to “damage” to a device—either damage “intended via a virus on the application or ... unintended where the application executes with poorly written code that unintentionally dominates a resource and makes it unavailable or damaged to other applications.” (Sprigg, 1:45-52.) Frank indicates that by allowing an administrator to view the “ramifications” of the selected security policies, its system allows the administrator to “make better decisions when defining a security profile.” (Frank, [0036].) Accordingly, a POSITA would have been motivated to

implement a security application for an administrator on user terminals in the Hayes-Sprigg combination.

309. A POSITA would have been further motivated to implement an administrator security application on a user terminal in the combined Hayes-Sprigg system because of the fact that formulating security policy for a computer network requires a balancing approach that is fundamentally iterative. For example, Frank discloses that “the degree to which the computer system is locked down by the security application depends on the competing interests of system security and system compatibility.” (Frank, [0008].) A POSITA would have understood that navigating such competing interests of setting a security policy would be best suited by seeing the results of such a policy in real time, as Frank’s system (and the combination between Hayes, Sprigg, and Frank) allows.

310. A POSITA would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques without undue experimentation. The Hayes, Sprigg, and Frank combination is standard computing technology. The proposed combination would have involved nothing more than the routine implementation of known techniques.

311. Frank, like Hayes and Sprigg, is analogous art to the ’571 patent. It is

also related to a networked computer system, managed by system administrators, as explained above. (Frank, [0002], [0029], [0008], [0005]-[0007], [0009]-[0012].)

(e) **“storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;”**  
(Claim 1[c])

312. It is my opinion that claim 1[c] is disclosed by or would have been obvious based on Hayes, or based on Hayes and Sprigg.

313. Hayes discloses that the administrator-provided information, including allowed applications and application preferences, are provided to a password-protected server. For example, Hayes discloses that the page on the profile manager application for defining allowed applications for end users allows a user to “save all pending changes” by clicking File **1312** and then clicking save. (Hayes, [0085]; *see also id.*, Figs. 17, 24 (showing File **1312** and indicating “Changes not saved!”), [0042] (“create, save, and retrieve the configuration information for software from permanent storage”), [0055], [0060], [0065], [0067].) Hayes discloses that saved information is sent to the database **212** on the server. (*Id.*, [0081], [0060], Figs. 5, 6, 11.)

314. Since the server database is password protected, as I discussed above, saving the owner control information via the profile manager application to the

server database is **“storing, by the electronic device, the owner control information in a protected data store to prevent alteration or deletion of the owner control information.”** Alteration or deletion is prevented for non-administrator users (*e.g.*, end users) who do not have administrative credentials. Further, this is **“in response to authenticating the owner control information using the owner information,”** because as discussed above, the administrator cannot access the profile manager for viewing or modifying owner control information unless administrative credentials (user ID and password) are provided. (Hayes, [0073], [0075], [0076], [0080], [0082], Figs. 7-11.)

315. The '571 patent shows that a password-protected database constitutes a **“protected data store.”** For example, the “owner control information store ... may be a remote data store accessible to the insertion tool, a local store, or some form of memory reader.” ('571, 10:47-51; 13:46-51 (“protected memory areas” where “[c]onfiguration may be used where only the insertion module **44** has write and erase access to these stores”), 20:3-10 (“The owner control information .... can be maintained on a remote server managed by the device owner. The remote server can maintain a device data store, that may be in the form of a database, that stores the control information, including application control information, associated with owned devices.”), 21:8-10 (“A remote server can be used to store owner control

information associated with one or more electronic devices, or groups of devices.”);  
22:59-60 (“The owner control information store can reside ... on one or more remote  
servers.”).)

### **Obviousness over Hayes and Sprigg**

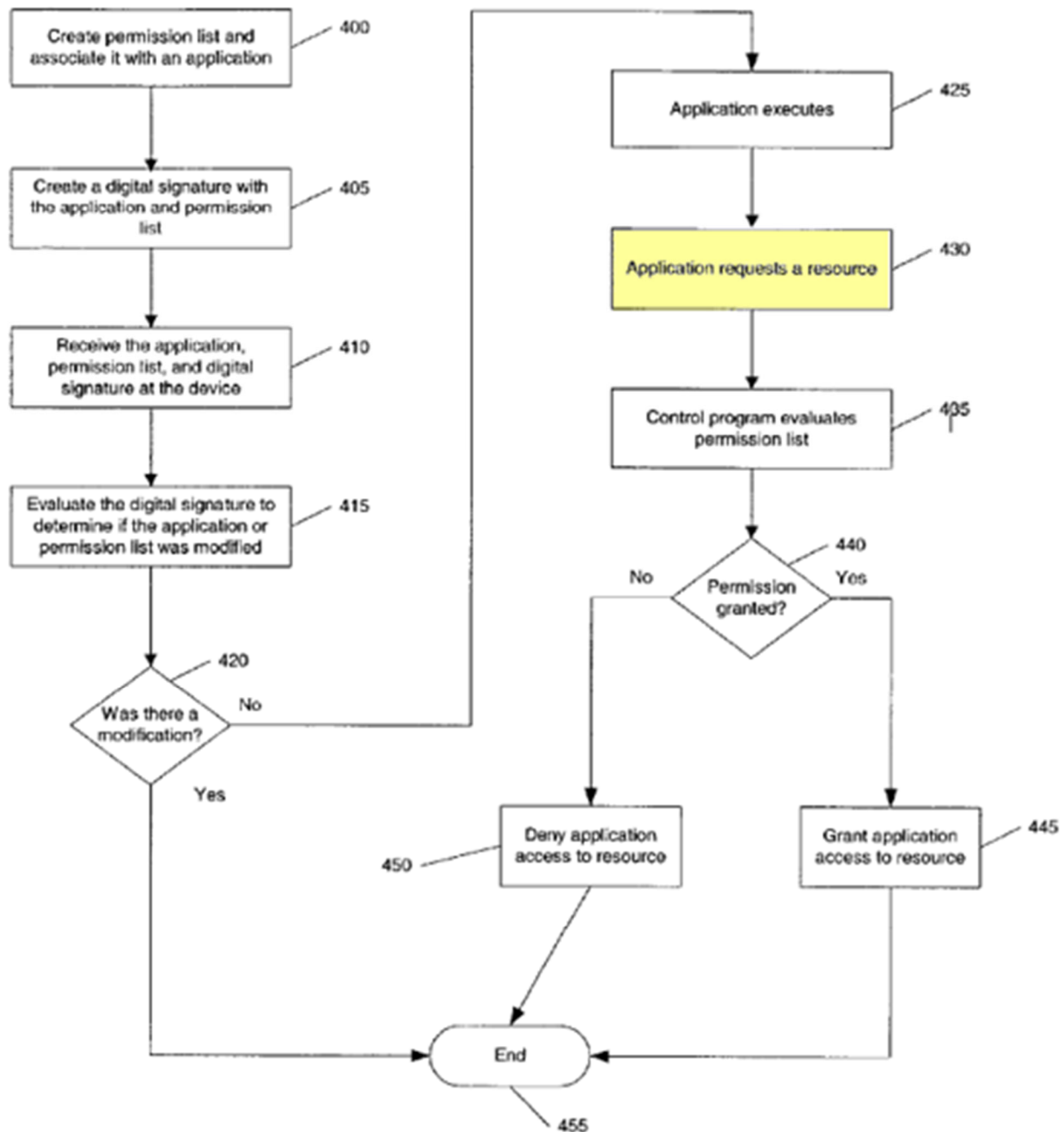
316. Further, it would have been obvious to a POSITA based on Sprigg that after a user terminal receives “**owner control information**,” a user would be restricted from modifying that information. For example, Sprigg discloses that one of the goals of its system is “protecting the resources of a device and the connected network,” due, for example, to the threat of damage caused by an application on a device or the network. (Sprigg, 1:45-52 (“This damage may be intended via a virus on the application or may be unintended where the application executes with poorly written code that unintentionally dominates a resource and makes it unavailable or damaged to other applications.”).) Accordingly, Sprigg discloses that its system checks whether permission information was modified before executing an application being checked against the permission information. (*Id.*, Fig. 4, 4:33-37, 5:25-38, 6:22-33, 6:51-7:23.) If it is determined that the permission information was modified (for example, on the basis of a digital signature), then Sprigg discloses preventing the application from executing. (*Id.*) Thus, the combined system could store “**owner control information**” in a “**protected data store to prevent**

**alteration or deletion of the owner control information”—i.e., prevent alteration**  
by preventing applications from executing if alteration is detected.

(f) **“receiving, by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 1[d])**

317. It is my opinion that claim 1[d] would have been obvious over Hayes in light of Sprigg.

318. As I discussed above, Sprigg discloses that in enforcing application permissions, a computer **“receiv[es], by the electronic device, from an application operating on the electronic device, a request to access local memory on the electronic device.”** For example, Sprigg discloses that an “application executes on [a wireless device] (Step 425).” (Sprigg, 7:20-23.) In doing so, the application “requests a resource on the device (Step 430)—i.e., the device **“receiv[es], by the electronic device, from an application operating on the electronic device, a request to access”** a resource. (*Id.*, 7:24-28.) This process is shown in Figure 4 of Sprigg, reproduced below:



(*Id.*, Fig. 4 (highlighting added).)

319. Sprigg discloses that the resource request can be a request to the local memory of the device—*i.e.*, the request can be “**a request to access local memory**”

**on the electronic device.”** (Sprigg, 4:25-32 (“the application may request access to memory”), 4:14-21 (“Examples of a device’s resources **120** include memory, including primary and secondary storage [and] files stored in memory, including the read, write and modify operations on such files[.]”), 1:37-41 (“Applications, during execution, require various resources on the device they are executing. These resources include memory (including primary and secondary storage)[.]”).)

320. As discussed above, it would have been obvious to implement Hayes’s system according to Sprigg, such that a device receives application permissions associated with allowed applications from a network administrator, and these permissions are enforced by receiving resource requests from applications, checking them against the relevant permission lists, and controlling application access accordingly.

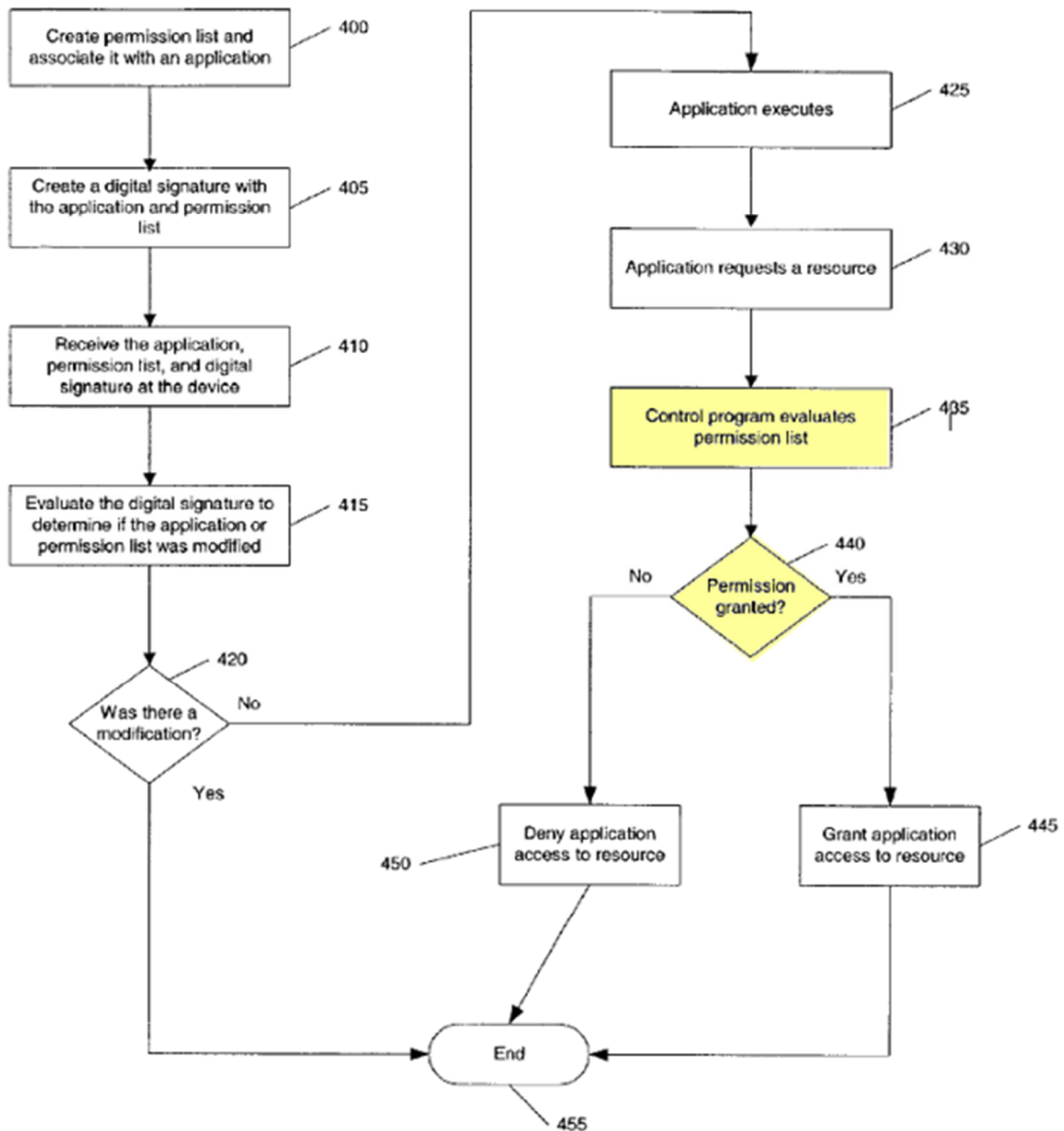
**(g) “determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 1[e])**

321. It is my opinion that claim 1[e] would have been obvious over Hayes in light of Sprigg.

322. As I discussed above, Sprigg discloses that in response to an application resource request (including a local memory request), a control program on a wireless device “evaluates and the permission list associated with the application” and

determines “[i]f the permission list indicates that the application has the privilege to access the requested resource (Step 440)” or “[i]f the permission list indicates that the application does not have the privilege to access the requested resource in Step 440[.]” (Sprigg, 7:30-44; *see also id.*, 4:25-32 (“the application may request access to memory”).) Thus, Sprigg discloses “**determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information[.]**”

This process is shown in Figure 4 of Sprigg, reproduced below:



(*Id.*, Fig. 4 (highlighting added).)

323. As discussed above, it would have been obvious to implement Hayes's system according to Sprigg, such that a device receives application permissions

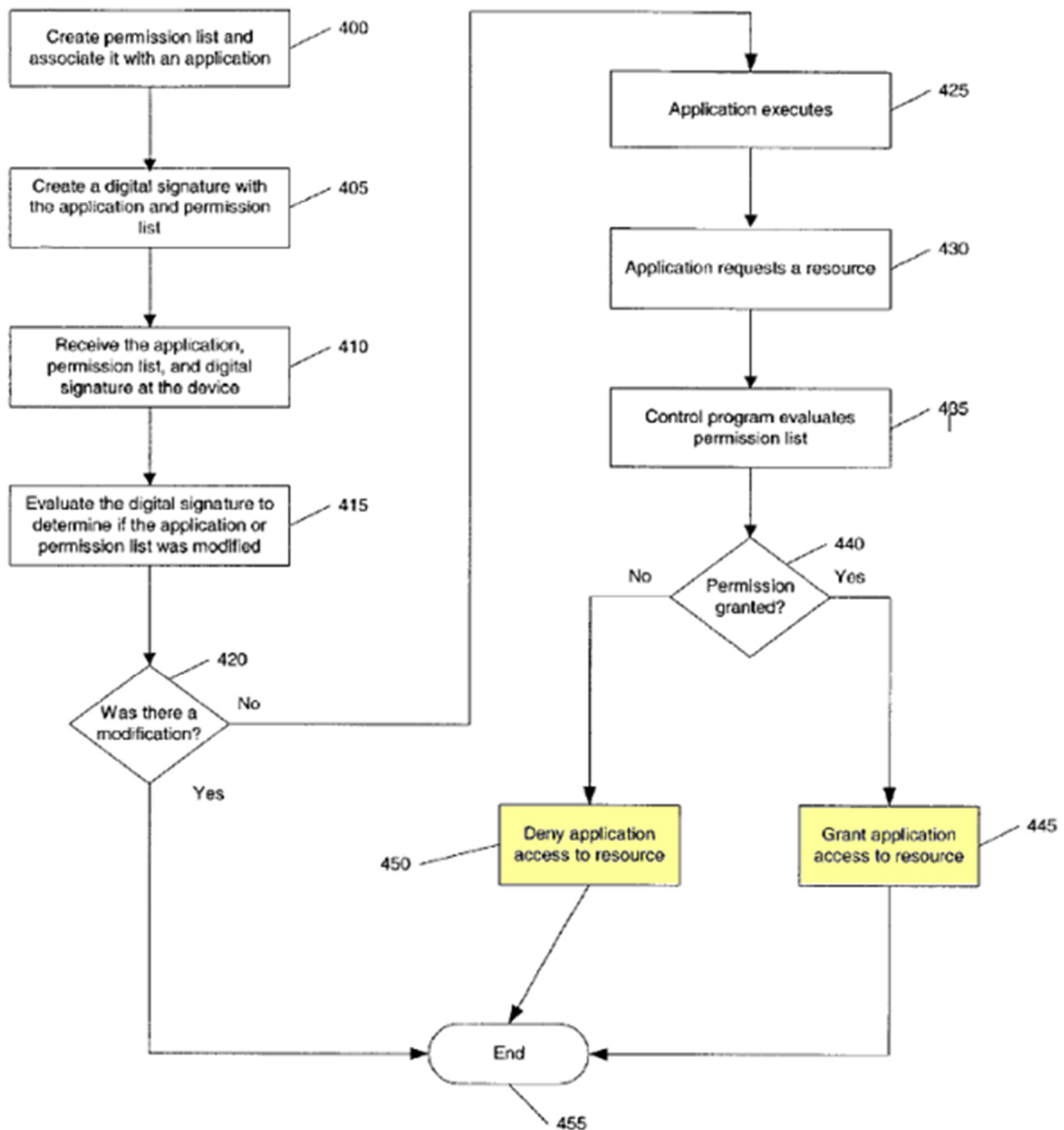
associated with allowed applications from a network administrator, and these permissions are enforced by receiving resource requests from applications, checking them against the relevant permission lists, and controlling application access accordingly.

**(h) “controlling application access to the local memory based upon the determining.” (Claim 1[f])**

324. It is my opinion that claim 1[f] would have been obvious over Hayes in light of Sprigg.

325. As I discussed above, Sprigg discloses that after determining whether an application’s access to a resource (including local memory) is allowed based on the relevant permissions list, the wireless device either prevents or allows the application to access the resource—thereby **“controlling application access to the local memory based upon the determining.”** For example, Sprigg discloses that “[i]f the permission list indicates that the application has the privilege to access the requested resource (Step **440**), the application will be granted access to the resource (Step **445**).” (Sprigg, 7:30-34.) Sprigg discloses that “[i]f the permission list indicates that the application does not have the privilege to access the requested resource in Step **440**, then the request to access the resource is denied (Step **450**).” (*Id.*, 7:35-44 (disclosing “allowing execution to continue but without access to the resource”).) These processes of controlling resource access based upon the

“**determining**” of application access from permissions is shown in Sprigg’s  
Figure 4, reproduced below:



(*Id.*, Fig. 4 (highlighting added), 7:30-44.)

326. As discussed above, it would have been obvious to implement Hayes's system according to Sprigg, such that a device receives application permissions associated with allowed applications from a network administrator, and these permissions are enforced by receiving resource requests from applications, checking them against the relevant permission lists, and controlling application access accordingly.

327. It is thus my opinion that claim 1 is obvious over Hayes in view of Sprigg. Alternatively, claim 1 is obvious in view of Hayes, Sprigg, Frank, and Guedalia.

## **2. Dependent claim 2**

328. For reference, claim 2 recites:

2. The method of claim 1, wherein the request to access the local memory comprises a request to erase data from the local memory.

('571, 29:30-32 (Claim 2).)

329. It is my opinion that claim 2 is obvious over Hayes in view of Sprigg. Claim 2 is satisfied by both Grounds 3 and 4.

330. As explained above in claim 1[d], Sprigg discloses a system for managing application access to the resources on a computer. (Sprigg, 4:14-21, 4:25-32, 4:34-42, 7:24-43, Figs. 1, 4.) Sprigg discloses that the resources that can be

controlled by its system include “files stored in memory, including the read, write and modify operations on such files[.]” (*Id.*, 4:14-19, 4:25-27, 4:34-37.) Since “write and modify operations” on a file entail “eras[ing] data” (*i.e.*, erasing the data overwritten by the write or modify operation), Sprigg discloses “**the request to access the local memory comprises a request to erase data from the local memory.**”

331. Accordingly, since it would have been obvious to implement Hayes’s system using the application resource access management system disclosed by Sprigg, it is my opinion that it would have been obvious to implement Hayes’s system such that “**the request to access the local memory comprises a request to erase data from the local memory.**”

### 3. Dependent claim 3

332. For reference, claim 3 recites:

3. The method of claim 1, wherein the request to access the local memory comprises a request to read data from the local memory.

(’571, 29:33-35 (Claim 3).)

333. It is my opinion that claim 3 is obvious over Hayes in view of Sprigg. Claim 3 is satisfied by both Grounds 3 and 4.

334. As explained above in claims 1[d] and 2, Sprigg discloses a system for

managing application access to the resources on a computer. (Sprigg, 4:14-21, 4:25-32, 4:34-42, 7:24-43, Figs. 1, 4.) Sprigg discloses that the resources that can be controlled by its system include “files stored in memory, including the read, write and modify operations on such files[.]” (*Id.*, 4:14-19 (emphasis added), 4:25-27, 4:34-37.) Since Sprigg discloses managing the “read” operations on files stored in memory, Sprigg discloses **“the request to access the local memory comprises a request to read data from the local memory.”**

335. Accordingly, since it would have been obvious to implement Hayes’s system using the application resource access management system disclosed by Sprigg, it is my opinion that it would have been obvious to implement Hayes’s system such that **“the request to access the local memory comprises a request to read data from the local memory.”**

#### **4. Dependent claim 4**

336. For reference, claim 4 recites:

4. The method of claim 1, further comprising restricting modification of the owner control information after the owner control information has been stored in the protected data store.

(’571, 29:36-39 (Claim 4).)

337. It is my opinion that claim 4 is disclosed by Hayes or obvious over the combination of Hayes and Sprigg. Claim 4 is satisfied by both Grounds 3 and 4.

338. Hayes discloses that the administrator-provided information, including allowed applications and application preferences, are provided to a password-protected server. For example, Hayes discloses that the page on the profile manager application for defining allowed applications for end users allows a user to “save all pending changes” by clicking File **1312** and then clicking save. (Hayes, [0085]; *see also id.*, Figs. 17, 24 (showing File **1312** and indicating “Changes not saved!”), [0042] (“create, save, and retrieve the configuration information for software from permanent storage”), [0055], [0060], [0065], [0067].) Hayes discloses that saved information is sent to the database **212** on the server. (*Id.*, [0081], [0060], Figs. 5, 6, 11.)

339. Since the server database is password protected, as I discussed above in claim 1[c], Hayes’s system “**restrict[s] modification of the owner control information after the owner control information has been stored in the protected data store[.]**” Alteration or deletion is prevented for non-administrator users (*e.g.*, end users) who do not have administrative credentials. The administrator cannot access the profile manager for viewing or modifying owner control information unless administrative credentials (user ID and password) are provided. (Hayes, [0073], [0075], [0076], [0080], [0082], Figs. 7-11.) Further, it would have been obvious to a POSITA based on Sprigg that after a user terminal receives

application permission information like Sprigg discloses, a user would be restricted from modifying that information. For example, Sprigg discloses that one of the goals of its system is “protecting the resources of a device and the connected network,” due, for example, to the threat of damage caused by an application on a device or the network. (Sprigg, 1:45-52 (“This damage may be intended via a virus on the application or may be unintended where the application executes with poorly written code that unintentionally dominates a resource and makes it unavailable or damaged to other applications.”).) Accordingly, Sprigg discloses that its system checks whether permission information was modified before executing an application being checked against the permission information. (*Id.*, Fig. 4, 4:33-37, 5:25-38, 6:22-33, 6:51-7:23.) If it is determined that the permission information was modified (for example, on the basis of a digital signature), then Sprigg discloses preventing the application from executing. (*Id.*) Thus, the combined system **“restrict[s] modification of the owner control information [*i.e.*, prevents modification without consequences to the execution of applications] after the owner control information has been stored in the protected data store[.]”**

**5. Dependent claim 5**

340. For reference, claim 5 recites:

5. The method of claim 1, wherein the owner control information includes an authorization record and an application identifier for

each of the applications, and the owner control information is provided by an external source through a wireless communication channel.

(’571, 29:40-44 (Claim 5).)

341. It is my opinion that claim 5 would have been obvious over Hayes in light of Sprigg. Claim 5 is satisfied by both Grounds 3 and 4.

342. Hayes discloses that the “**owner control information is provided by an external source.**” Hayes discloses that a server (including servlet **214**) provides the “**list of applications permitted for installation**” discussed above. (Hayes, [0071] (“The ProfileManagmentProperties object P requests the information at **802** from the profile manager servlet **214**, which generates a response with the requested information at **804.**”), Fig. 8.) Thus, Hayes discloses that the “**owner control information is provided by an external source** [*e.g.*, a server]”.

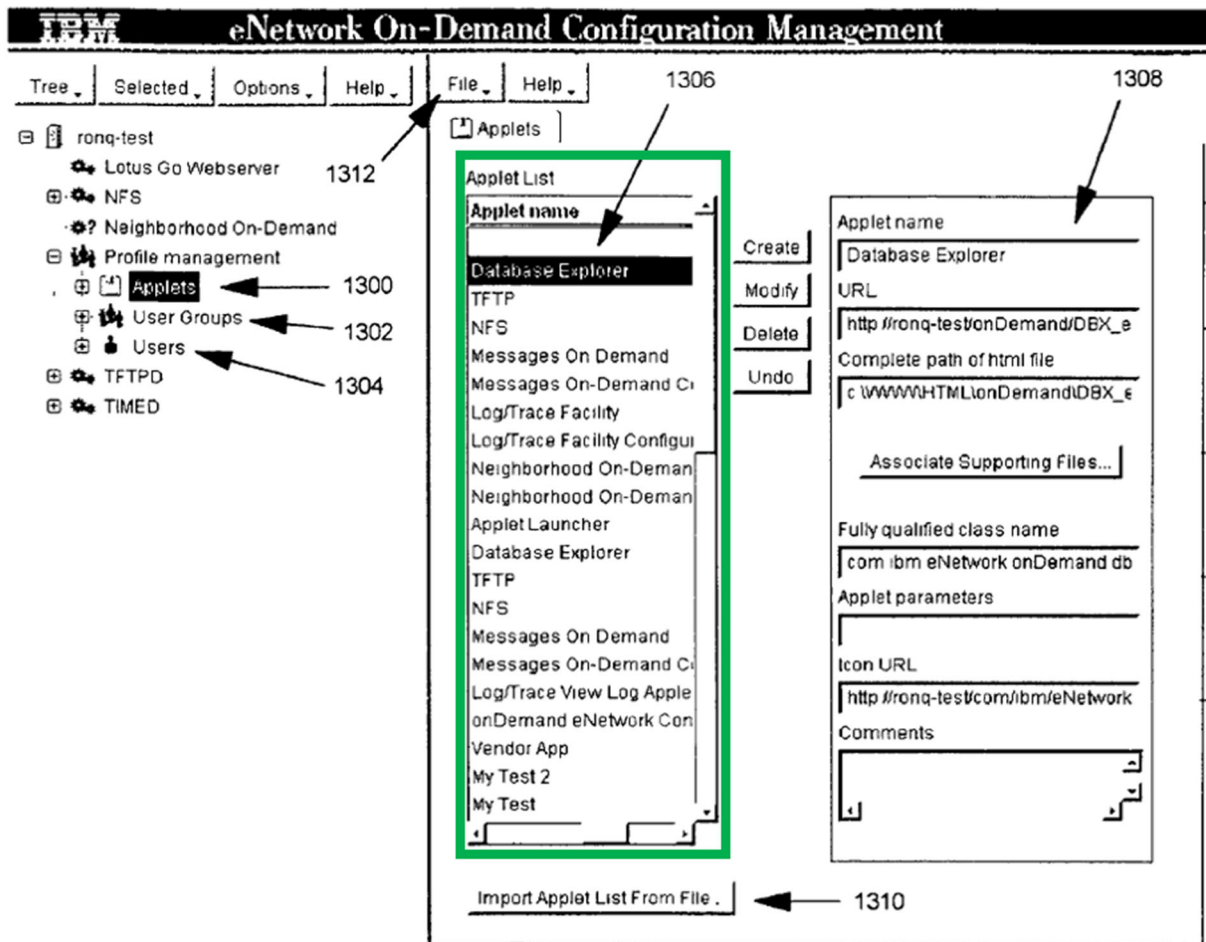
343. Further, Hayes discloses that the “**owner control information is provided ... through a wireless communication channel.**” Hayes discusses that its system is used with a network of computers connected via a “local area network” or “wide area networking.” (Hayes, [0037], Fig. 1.) A POSITA would have understood that local area or wide area networks could include wireless communication channels like Wi-Fi. (*Id.*, Fig. 1 (representing network **100** as a

cloud); EX1015 (Donald D. Spencer, *Spencer's Illustrated Computer Dictionary* (1995)), p.006 (defining “wide area network” as “generally implemented by linking together several remote Local Area Networks (LANs) through the use of gateways and bridges over dedicated telephone lines, satellite dishes or radio waves”).) Further, this would have been obvious based on Sprigg, which discloses the use of “wireless devices” and “a wireless RF network” with its system. (Sprigg, 4:46-51; *see also id.*, 4:52-5:38 (discussing system comprising server and wireless devices), 5:39-53, Figs. 1-3.) A POSITA would have been motivated to use a “**wireless communication channel**” in Hayes’s system to enable the use of its network with as many types of devices as possible, including mobile devices without a wired connection. (*See, e.g.*, Hayes, [0037] (disclosing use of its system with “mobile laptop computers **104**” and that “[t]here is no intent to limit the environment in which the invention might be practiced; indeed, a network of any type that interconnects many types of stations is envisioned”).)

344. The limitation “**the owner control information includes an authorization record and an application identifier for each of the applications**” would have been obvious over Hayes in view of Sprigg (EX1012; U.S. Patent No. 7,743,407). As I explained above, Hayes discloses an interface via which a network administrator can determine whether applications are allowed for different

users on an application-by-application basis. For example, in Figure 13, Hayes shows an “Applet List” with options for an administrator to “Create” or “Delete” applets:

Fig. 13



(Hayes, Fig. 13 (highlighting added), [0085].) Further, Hayes discloses a screenshot of an interface where an administrator can allow a subset of permitted applications for a particular user (Figure 24), or for groups of users (Figure 17):

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

Fig. 24

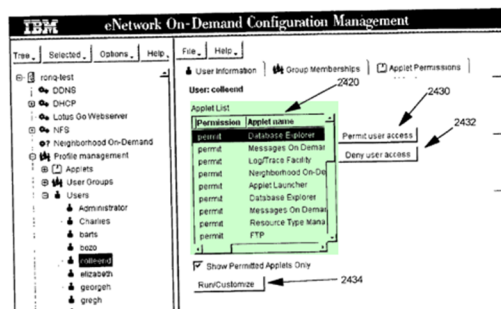
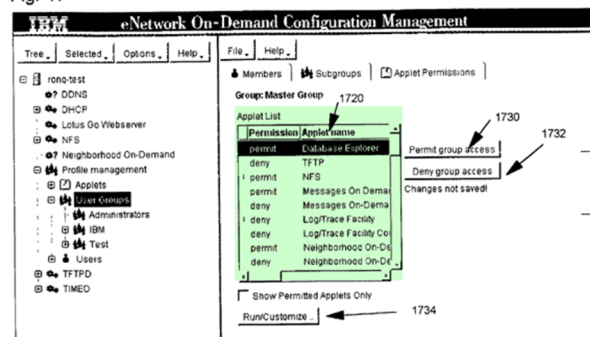


Fig. 17



(*Id.*, Figs. 24 & 17 (highlighting added), [0093], [0088].)

345. Further, Hayes teaches that when an end user brings up the desktop on a terminal, the “desktop objects calls a method ... to get a list of the software to which the user has access permission.” (Hayes, [0071] (emphasis added).)

346. Hayes discloses that the server provides “a user friendly name, the applet’s URL, the URL of an icon for the applet, etc. (information that is required for the desktop to represent the applet on the desktop and to load and launch it.” (Hayes, [0071] (emphasis added).)

347. Moreover, “the server stores a plurality of user applications for downloading to user stations and further stores access permissions for the applications.” (Hayes, [0013]) (emphasis added).) Hayes explains that the server uses a user’s identifying information to “build a list of applications for which the user has access permission.” (*Id.*) The server further “downloads to the station a list of applications to which the user has access permission,” and “[t]he user station

uses the list to build a folder containing only the applications from the list to which the user has access permission.” (*Id.*; *see also id.*, claim 1 (reciting “downloading to the station the list of applications for which the user has access permissions” and requesting “a download of the corresponding application to the user station”).)

348. Thus, Hayes alone discloses that **“the owner control information includes ... an application identifier for each of the applications.”**

349. Further, as I explained above, Sprigg discloses a computer network where a wireless device **300** contains “applications **310** each with a permission list **320**.” (Sprigg, 5:41-43.) Sprigg discloses that “each application [**310**]<sup>5</sup> may have a separate permission list associated with that application[.]” (*Id.*, 5:45-48.) Sprigg further discloses that these permissions associated with each application “contain[] a listing of the resources **315** and an indication whether the application has permission to access any of the specific resources **315** on the device.” (*Id.*, 5:63-66.) For example, Sprigg discloses that the permission lists can control access to

---

<sup>5</sup> The specification in Sprigg indicates “application **110**.” (Sprigg, 5:45.) However, a POSITA would have understood that this is a typo and should refer to “application [**310**],” consistent with the numbering of Figure 3 and the surrounding discussion in the specification. (*Id.*, Fig. 3, 5:39-53.)

“memory, including primary and secondary storage” and “files stored in memory, including the read, write and modify operations on such files.” (*Id.*, 4:14-21.) Thus, Sprigg discloses that **“the owner control information includes an authorization record.”**

350. As I also explained above, it would have been obvious to modify Hayes’s administrator interface program (shown in, *e.g.*, Hayes’s Figs. 13, 17, and 24) in light of Sprigg to allow an administrator to provide application resource restrictions on an application-by-application basis. This would have led to the server providing a client device **“owner control information”** including **“an authorization record and an application identifier for each of the applications.”**

351. For example, Hayes discloses that a user terminal receives from the server a “list of the software to which the user has access permission” including “a user friendly name, the applet’s URL, the URL of an icon for the applet, etc. (information that is required for the desktop to represent the applet on the desktop and to load and launch it).” (Hayes, [0071] (emphasis added).) This information includes various **“application identifier[s]”**—including the name and URL of the applet. (*Id.*; *see also* Sprigg, 5:25-28 (“The application, in one embodiment, has a unique identifier to distinguish it from other applications.”), Fig. 3.) Further, in the combination of Hayes and Sprigg, the **“application identifier”** information would

be paired with an **“authorization record”**—*e.g.*, the resource access restriction information disclosed by Sprigg. (Sprigg, 5:41-43, 5:45-48, 5:63-66.)

**6. Dependent claim 6**

352. For reference, claim 6 recites:

6. The method of claim 5, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

(’571, 29:45-49 (Claim 6).)

353. It is my opinion that claim 6 would have been obvious over Hayes in view of Sprigg. Claim 6 is satisfied by both Grounds 3 and 4.

354. As I explained above in claim 1[e], it would have been obvious for Hayes’s system to provide **“owner control information”** including an **“authorization record related to determining whether access to the local memory is allowed.”** Sprigg discloses providing permission lists for applications that can control access to “memory, including primary and secondary storage” and “files stored in memory, including the read, write and modify operations on such files.” (Sprigg, 4:14-21.) It would have been obvious for the server in Hayes’s system to provide such permission lists on an application-by-application basis, thereby providing an **“authorization record related to determining whether**

**access to the local memory is allowed.”**

355. Hayes discloses that the “**owner control information**” is “**provided by an external computer.**” Hayes discloses that a server (including servlet **214**) provides the owner control information. (Hayes, [0071] (“The ProfileManagmentProperties object P requests the information at **802** from the profile manager servlet **214**, which generates a response with the requested information at **804**.”), Fig. 8.) Thus, Hayes discloses that the “**owner control information is provided by an external computer** (*e.g.*, a server).”

356. Hayes discloses that the external computer is “**used to enforce policies for operating electronic devices within an organization.**” Hayes contemplates use of its system in a business organization. For example, Hayes discloses using its system for enforcing policies on a “corporate intranet.” (Hayes, [0001], [0002] (“the software administration problems that attend large numbers of corporate users will be substantially reduced”).) Further, when discussing the implementation of group permissions, Hayes discloses that such permissions reflect “enterprise modeling”—in other words, the structure of an organization. (*Id.*, [0059].)

357. Accordingly, it is my opinion that claim 6 is obvious over Hayes in view of Sprigg.

**7. Dependent claim 7**

358. For reference, claim 7 recites:

7. The method of claim 1, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

(’571, 29:50-52 (Claim 7).)

359. It is my opinion that claim 7 is disclosed by Hayes. Claim 7 is satisfied by both Grounds 3 and 4.

360. Hayes discloses **“an update to the owner control information is provided.”** Hayes discloses that each time a user logs onto the system, the server is checked for the **“list of applications permitted for installation,”** and updated information is sent to the user’s terminal, which is used to build the desktop. Hayes discloses that “[w]hen a user attempts to log onto the system, the server uses the user’s log-on identifier to build a list of applications for which the user has access permission.” (Hayes, Abstract; *see also id.*, [0012] (“When the user logs onto the system, the user identifies him or herself to the server by means of a system identifier and a password. The server uses this information to built [sic] dynamically a list of applications to which the user has access permission.”), [0004].) Hayes discloses that a user’s terminal “reads its preference information out of its ProfileManagementProperties object P, and begins to update the desktop

accordingly.” (*Id.*, [0071] (emphasis added).)

361. As discussed above in claims 5 and 6, the **“update to the owner control information is provided by an external source.”** Hayes discloses that a server (including servlet **214**) provides the owner control information. (Hayes, [0071] (“The ProfileManagmentProperties object P requests the information at **802** from the profile manager servlet **214**, which generates a response with the requested information at **804**.”), Fig. 8.) Thus, Hayes discloses that an **“update to the owner control information is provided by an external source [e.g., a server]”**.

362. Hayes discloses that the update to the owner control information is **“for storage on the electronic device.”** Hayes discloses that the owner control information is “stored in the ProfileManagementProperties object P, and returned to the desktop object” on the user terminal. (Hayes, [0071], Abstract (“The server downloads to the station a list of applications to which the user has access permission. The user station uses the list to build a folder containing only the applications from the list to which the user has access permission.”), [0012] (“The server uses this information to built dynamically a list of applications to which the user has access permission. That list is transmitted to the users station. The application list is then used to build a portion of the desktop, preferably a desktop folder, of applications to which the user has access permission.”), Figs. 7-8.) The

user terminal subsequently uses the stored information “to build a folder for the applets and to generate a window displaying the icons and the user friendly name for each applet to which the user has access.” (*Id.*, [0071].)

363. Accordingly, it is my opinion that claim 7 is disclosed by Hayes.

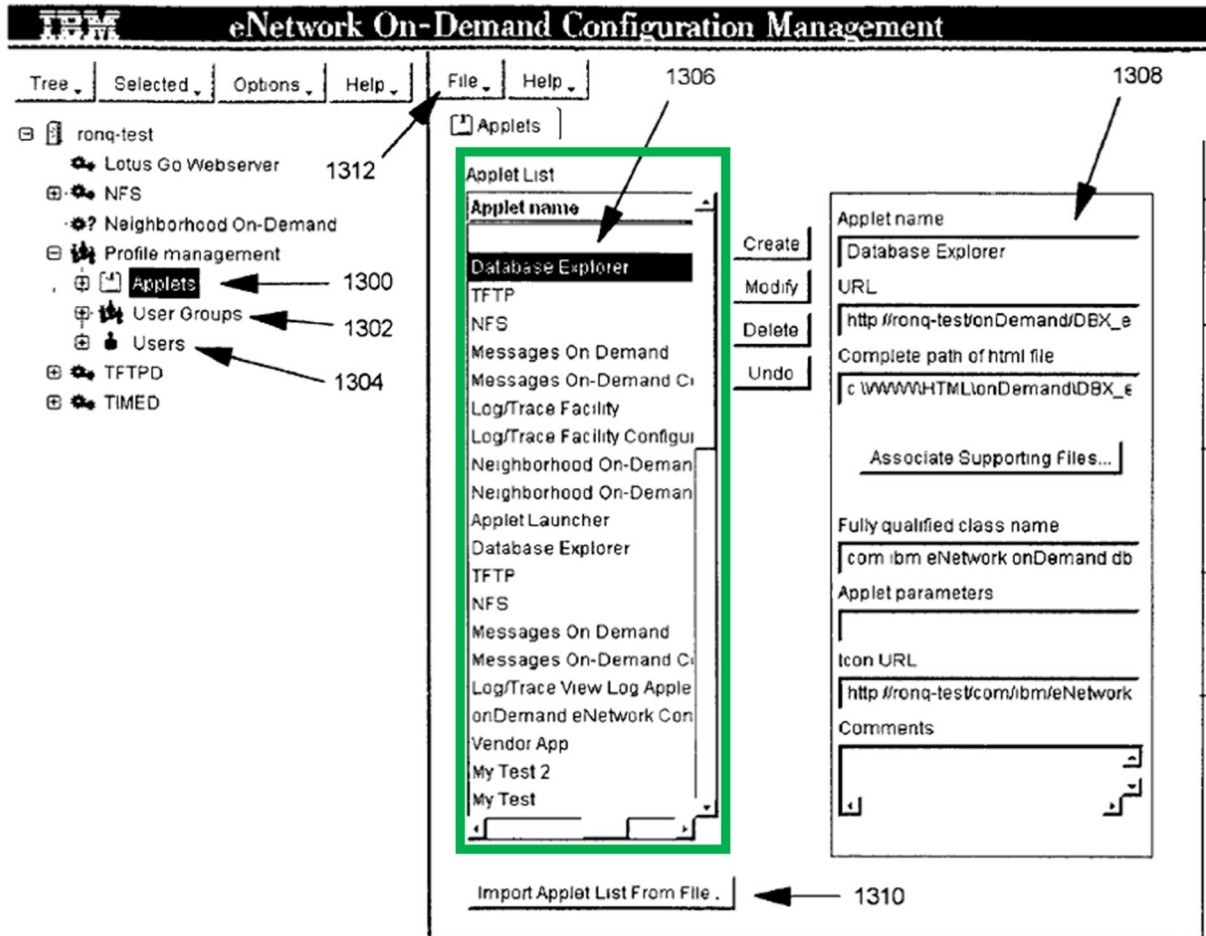
#### 8. Dependent claim 8

- (a) **“The method of claim 1, wherein a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device, the method further comprising:” (Claim 8[p])**

364. To the extent the preamble of claim 8 is limiting, it is obvious over Hayes in view of Sprigg. Claim 8 is satisfied by both Grounds 3 and 4.

365. As discussed above for claim 5, the limitation **“a plurality of authorization records associated with a plurality of application identifiers are stored on the electronic device”** would have been obvious over Hayes in view of Sprigg (EX1012; U.S. Patent No. 7,743,407). As I explained above, Hayes discloses an interface via which a network administrator can determine whether applications are allowed for different users on an application-by-application basis. For example, in Figure 13, Hayes shows an “Applet List” with options for an administrator to “Create” or “Delete” applets:

Fig. 13



(Hayes, Fig. 13 (highlighting added), [0085].) Further, Hayes discloses a screenshot of an interface where an administrator can allow a subset of permitted applications for a particular user (Figure 24), or for groups of users (Figure 17):

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

Fig. 24

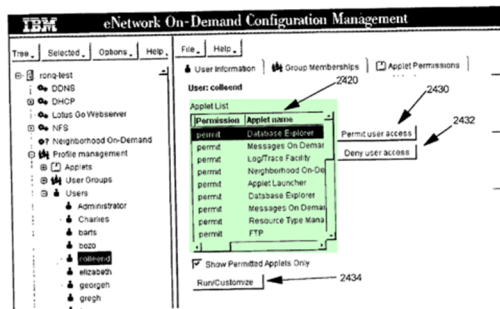
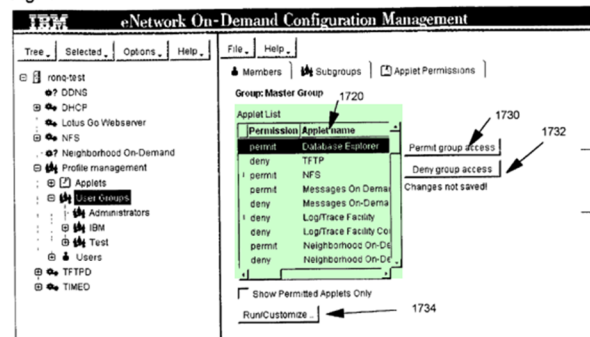


Fig. 17



(*Id.*, Figs. 24 & 17 (highlighting added), [0093], [0088].)

366. Further, Hayes teaches that when an end user brings up the desktop on a terminal, the “desktop objects calls a method ... to get a list of the software to which the user has access permission.” (Hayes, [0071] (emphasis added).)

367. Hayes discloses that the server provides “a user friendly name, the applet’s URL, the URL of an icon for the applet, etc. (information that is required for the desktop to represent the applet on the desktop and to load and launch it.” (Hayes, [0071] (emphasis added).)

368. Moreover, “the server stores a plurality of user applications for downloading to user stations and further stores access permissions for the applications.” (Hayes, [0013]) (emphasis added).) Hayes explains that the server uses a user’s identifying information to “build a list of applications for which the user has access permission.” (*Id.*) The server further “downloads to the station a list of applications to which the user has access permission,” and “[t]he user station

uses the list to build a folder containing only the applications from the list to which the user has access permission.” (*Id.*; *see also id.*, claim 1 (reciting “downloading to the station the list of applications for which the user has access permissions” and requesting “a download of the corresponding application to the user station.”).)

369. Thus, Hayes alone discloses that “**a plurality of authorization records ... are stored on the electronic device.**”

370. Further, as I explained above, Sprigg discloses a computer network where a wireless device **300** contains “applications **310** each with a permission list **320.**” (Sprigg, 5:41-43.) Sprigg discloses that “each application [**310**]<sup>6</sup> may have a separate permission list associated with that application[.]” (*Id.*, 5:45-48.) Sprigg further discloses that these permissions associated with each application “contain[] a listing of the resources **315** and an indication whether the application has permission to access any of the specific resources **315** on the device.” (*Id.*, 5:63-66.) For example, Sprigg discloses that the permission lists can control access to

---

<sup>6</sup> The specification in Sprigg indicates “application **110.**” (Sprigg, 5:45.) However, a POSITA would have understood that this is a typo and should refer to “application [**310**],” consistent with the numbering of Figure 3 and the surrounding discussion in the specification. (*Id.*, Fig. 3, 5:39-53.)

“memory, including primary and secondary storage” and “files stored in memory, including the read, write and modify operations on such files.” (*Id.*, 4:14-21.) Thus, Sprigg discloses that **“a plurality of authorization records associated with a plurality of application identifiers .”**

371. As I also explained above, it would have been obvious to modify Hayes’s administrator interface program (shown in, *e.g.*, Hayes’s Figs. 13, 17, and 24) in light of Sprigg to allow an administrator to provide application resource restrictions on an application by application basis. This would have led to the server providing a client device **“a plurality of authorization records associated with a plurality of application identifiers .”**

372. For example, Hayes discloses that a user terminal receives from the server a “list of the software to which the user has access permission” including “a user friendly name, the applet’s URL, the URL of an icon for the applet, etc. (information that is required for the desktop to represent the applet on the desktop and to load and launch it).” (Hayes, [0071] (emphasis added).) This information includes various **“application identifiers”**—including the name and URL of the applet. (*Id.*; *see also* Sprigg, 5:25-28 (“The application, in one embodiment, has a unique identifier to distinguish it from other applications.”), Fig. 3.) Further, in the combination of Hayes and Sprigg, the **“application identifier[]”** information would

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

be paired with an “**authorization record**[]”—*e.g.*, the resource access restriction information disclosed by Sprigg. (Sprigg, 5:41-43, 5:45-48, 5:63-66.) It would be obvious for the “**a plurality of authorization records**” to be “**stored on the electronic device**,” as both Hayes and Sprigg disclose the “**application identifier**” and “**authorization record**” information being stored. (Hayes, [0071], Abstract (“The server downloads to the station a list of applications to which the user has access permission. The user station uses the list to build a folder containing only the applications from the list to which the user has access permission.”), [0012] (“The server uses this information to built dynamically a list of applications to which the user has access permission. That list is transmitted to the users station. The application list is then used to build a portion of the desktop, preferably a desktop folder, of applications to which the user has access permission.”), Figs. 7-8; Sprigg, 5:32-35 (“This digital signature may be bound to the application and permission list and stored on the wireless device either bound or separate[.]”), 6:66-7:5 (describing that “the application, permission list and the digital signature” is received by “downloading this information from a network or by installing it directly onto the device”), 6:10-12.)

373. Thus, to the extent the preamble of claim 8 is limiting, it is obvious over Hayes in view of Sprigg.

(b) “receiving requests to access the local memory from a plurality of applications operating on the electronic device;” (Claim 8[a])

374. It is my opinion that claim 8[a] would have been obvious over Hayes in light of Sprigg.

375. For purposes of my analysis, claim 8[a] is substantially the same as claim 1[d]. Therefore, for the reasons discussed above for claim 1[d], it is my opinion that claim 8[a] would have been obvious based on Hayes in view of Sprigg. Claim 8[a] additionally requires receiving requests from “**a plurality of applications.**” As I discussed above for claim 1[d], Sprigg discloses that its system receives requests from various applications (“**a plurality of applications**”). (Sprigg, 1:13-15 (“The present invention relates to processing of applications for use in a computer device, and more particularly, to the granting of device resources per application.”), 8:27-31 (“The user privilege level, while impacting the access to resources across all applications the user executes, does not provide the increased granularity of resource allocation as described herein and claimed by the present invention.” (emphasis added)), 5:41-45 (“It will be recognized by those skilled in the art the applications **310** may perform different tasks.”), 9:31-60.) Claim 8[a] is satisfied by both Grounds 3 and 4.

376. As discussed above, it would have been obvious to implement Hayes’s

system according to Sprigg, such that a device receives application permissions associated with allowed applications from a network administrator, and these permissions are enforced by receiving resource requests from applications, checking them against the relevant permission lists, and controlling application access accordingly.

- (c) **“determining whether access to the local memory is allowed to be performed by their respective applications based upon the stored authorization records and the application identifiers that are respectively associated with the plurality of applications; and:” (Claim 8[b])**

377. It is my opinion that claim 8[b] would have been obvious over Hayes in light of Sprigg.

378. As explained above for claims 1[e] and 6, Sprigg discloses determining local memory access based on policy rules, which (as discussed above for claim 8[p]) constitute **“stored authorization records and the application identifiers that are respectively associated with the plurality of applications.”** Thus, it is my opinion that claim 8[b] is obvious over Hayes in view of Sprigg. Claim 8[b] is satisfied by both Grounds 3 and 4.

379. As discussed above, it would have been obvious to implement Hayes’s system according to Sprigg, such that a device receives application permissions associated with allowed applications from a network administrator, and these

permissions are enforced by receiving resource requests from applications, checking them against the relevant permission lists, and controlling application access accordingly.

(d) **“controlling access by the plurality of applications to local memory based upon whether access to the local memory is allowed.” (Claim 8[c])**

380. It is my opinion that claim 8[c] would have been obvious over Hayes in light of Sprigg.

381. For purposes of my analysis, claim 8[c] is substantially the same as claim 1[f]. Therefore, for the reasons discussed above for claim 1[f], it is my opinion that claim 8[c] is disclosed by or would have been obvious based on Hayes in light of Sprigg. Claim 8[c] additionally requires controlling access by **“a plurality of applications.”** As I discussed above for claim 1[f], Sprigg discloses that its system controls local memory access for various applications (**“a plurality of applications”**). (Sprigg, 1:13-15 (“The present invention relates to processing of applications for use in a computer device, and more particularly, to the granting of device resources per application.”), 8:27-31 (“The user privilege level, while impacting the access to resources across all applications the user executes, does not provide the increased granularity of resource allocation as described herein and claimed by the present invention.” (emphasis added)), 5:41-45 (“It will be

recognized by those skilled in the art the applications **310** may perform different tasks.”), 9:31-60.) Claim 8[c] is satisfied by both Grounds 3 and 4.

382. As discussed above, it would have been obvious to implement Hayes’s system according to Sprigg, such that a device receives application permissions associated with allowed applications from a network administrator, and these permissions are enforced by receiving resource requests from applications, checking them against the relevant permission lists, and controlling application access accordingly.

**9. Dependent claim 9**

383. For reference, claim 9 recites:

9. The method of claim 8, wherein a group containing two or more of the applications is associated with one of the authorization records.

(’571, 30:1-3 (Claim 9).)

384. It is my opinion that claim 9 is obvious over Hayes in view of Sprigg and **Lambert** (EX1004; U.S. Patent App. Pub. 2002/0099952). Claim 9 is satisfied by Ground 5.

385. As discussed above, the combination of Hayes and Sprigg involves a system in which an administrator can set application access restrictions on an application-by-application basis. It would have been obvious based on Lambert to

allow certain applications to share access restrictions, such that **“a group containing two or more of the applications is associated with one of the authorization records.”**

386. Much like Hayes and Sprigg, Lambert discloses restricting access to device resources on an application-by-application basis. (Lambert, [0064]-[0065], [0068]-[0071], [0080], [0082].) Lambert discloses various examples of **“a group containing two or more of the applications”** having the same access restrictions.

387. For example, Lambert discloses that an access restriction can be associated with a filepath, such that any applications at that filepath have the same restrictions. (Lambert, [0058]-[0062], [0082], [0068], [0066].) Lambert discloses that filepath-based access restrictions are useful since they allow certain applications—for example, “system files” necessary to be allowed to run for the computer to “work normally”—to be treated in the same way by the access restriction system. (*Id.*, [0058].)

388. Lambert also discloses that an access restriction can be set using a “zone rule,” wherein “the zone identifies software according to the source (e.g., the URL zone or the like) from which it is downloaded or otherwise installed.” (Lambert, [0063].) Such “zone rules” represent another way Lambert discloses associating a group of applications with a single restriction level, so that “an

administrator can set different rules for software files classified according to their source.” (*Id.*)

389. Lambert also discloses an example access restriction policy in which multiple listings are associated with the same restriction level. (Lambert, [0082].) For example, the below excerpt shows that multiple entries are associated with the same “Disallowed” or “Unrestricted” access restriction level.

|                       |                                     |              |                |
|-----------------------|-------------------------------------|--------------|----------------|
| OnlySignedLockDown    | HKCU                                | Disallowed   | CP only        |
| Path                  | %windir%                            | Unrestricted | All file types |
| Certificate           | <publisher cert>                    | Unrestricted |                |
| IexploreOn-lyLockDown | HKCU                                | Disallowed   | CP only        |
| Path                  | %windir%                            | Unrestricted | All file types |
| Path                  | %programfiles%\Internet Explorer\   | Unrestricted | All file types |
| WMPOnlyLockDown       | HKCU                                | Disallowed   | CP Only        |
| Path                  | %windir%                            | Unrestricted | All file types |
| Path                  | %programfiles%\Windows Media Player | Unrestricted | All file types |
| PFNoMediaLockDown     | HKCU                                | Disallowed   | CP Only        |
| Path                  | %windir%                            | Unrestricted | All file types |
| Path                  | %programfiles%\                     | Unrestricted | All file types |
| Path                  | %programfiles%\Windows Media Player | Disallowed   | All file types |

(*Id.*) Lambert discloses that various “code authorization levels” can be defined, including “for unrestricted operation, one for end-user, one for constrained, one for untrusted and one for revoked[.]” (*Id.*, [0079], Fig. 7.) As shown in the example policy in Lambert, each of these “code authorization levels” can be shared by a group of applications. (*Id.*, [0082].)

390. It would have been obvious based on Lambert’s disclosures to implement the combined Hayes and Sprigg system such that **“a group containing two or more of the applications is associated with one of the authorization records”**—*i.e.*, multiple applications would be associated with the same access restriction level.

391. **Motivation to Combine:** Hayes, Sprigg, and Lambert are analogous art in a similar field. Each relates to administration and management of a computer network to limit application use by users. (Hayes, [0001] (“the invention relates to server-based storage of software preferences (configuration data) for software retrieved from a server and executing at the desktop computer”); Sprigg, 1:13-15 (“The present invention relates to ... the granting of device resources per application.”), 3:36-41 (indicating that “system administrator ... may create or provide input to creating this permission list for the application when used on the device”); Lambert, [0078] (“an administrator (possibly multiple administrators)

constructs the various policies [sic] that make up the effective policy 502”), [0002] (“The present invention is generally directed to computer systems, and more particularly to an improved security framework for computer systems.”), [0080]-[0081], [0003].) Furthermore, each reference relates to administering the network of a business enterprise. (Hayes, [0001] (discussing invention as relating to computers “connected to a network such as a corporate intranet”), [0059] (discussing “enterprise modeling”), [0002]; Sprigg, 1:20-24 (background of invention includes “businesses rely[ing] more on their wireless devices, such as mobile phones and personal digital assistants (PDAs)”); Lambert, [0003] (discussing “enterprise computing environments” where “administrators begin to lose control over what software code the enterprise’s machines are executing”), [0007] (“In sum, in contemporary computer systems, running unknown code cannot be prevented, and indeed is necessary to an extent in many enterprises, yet doing so leads to increased support costs in system maintenance and helpdesk time, and decreased user productivity.”), *id.* (discussing the “rise in the usage of networks, email and the Internet for business computing”).)

392. A POSITA would have been motivated to implement access restrictions shared across multiple applications to simplify and make more efficient the process of constructing policy restrictions for an administrator. For example, instead of

having to input separate access restriction rules for each application, an administrator could simply group applications—for example, based on filepath, zone, or other characteristics—and apply a common access restriction policy to the whole group. As a result, a POSITA would have recognized that administrator time would be saved and policies could be crafted more quickly in adapting to changing conditions or needs of users. (*See, e.g.*, Lambert, [0007] (referencing “increased support costs in system maintenance and helpdesk time, and decreased user productivity”).)

393. A POSITA would have been further motivated to implement access restrictions shared across multiple applications to facilitate more comprehensive access restriction policies that make it less likely that certain applications will be neglected or forgotten in the process. Allowing an administrator to make an access restriction policy for an entire filepath, for instance, prevents an application at that filepath from slipping through the cracks due to administrator error. A POSITA would have been motivated to favor broader security policies to prevent such circumstances. For example, Sprigg makes clear that any given application can “intentionally or unintentionally, degrade or corrupt other files on the wireless device or the network on which the wireless device communicates.” (Sprigg, 1:31-36.)

394. A POSITA would have been further motivated to implement access

restriction policies that could be shared across multiple applications to make the policies easier to adjust in real time. For example, in a system where access restriction policies can only be set on the basis of individual applications, if the administrator realizes that certain comprehensive changes need to be made (*e.g.*, access was generally granted/denied to a certain resource that is causing issues on a device or the network), then those changes will need to be made on an application-by-application basis. If instead, access restrictions could be shared between multiple applications, then the administrator could make the adjustment more easily—adjusting a single policy that is shared by multiple applications, rather than adjusting each individual policy for those applications. (*See, e.g.*, Lambert, [0007] (referencing “increased support costs in system maintenance and helpdesk time, and decreased user productivity”).)

395. A POSITA would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques without undue experimentation. Sprigg discloses that the prior art featured access restrictions that were the same across multiple applications—*e.g.*, based on the privileges of a user. (Sprigg, 1:61-2:2.) Accordingly, implementing access restrictions that are shared across different applications is simply using Sprigg’s system (application-by-application

restrictions) to implement a feature already in the prior art (restrictions shared by applications). The proposed combination would have involved nothing more than the routine implementation of known techniques.

396. Hayes, Sprigg, and Lambert are analogous art to the '571 patent for the same reasons as described above.

#### **10. Independent claim 10**

##### **(a) “A device, comprising:” (Claim 10[p])**

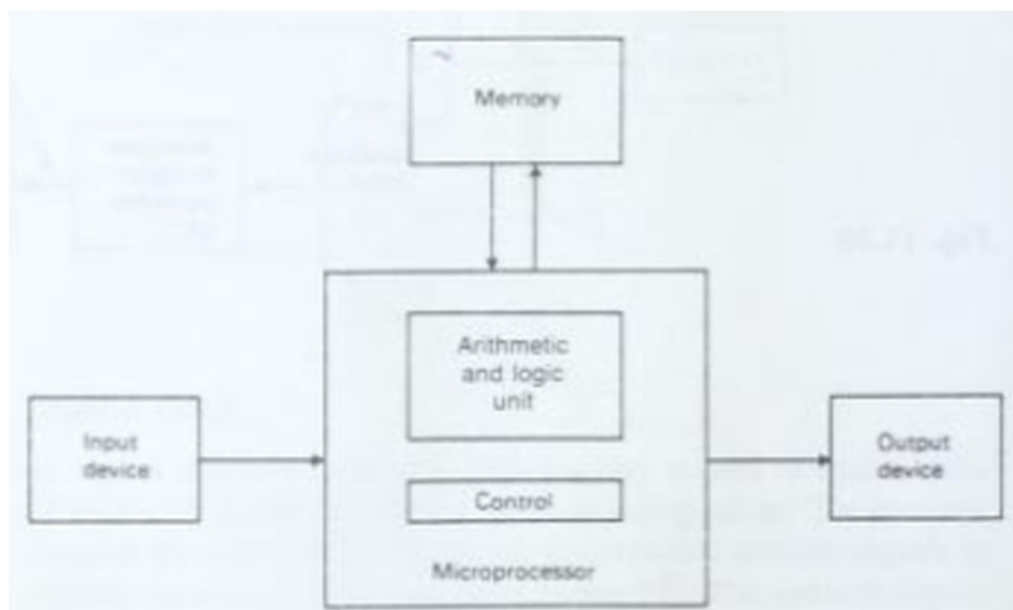
397. To the extent the preamble to claim 10 is limiting, it is my opinion that it is disclosed by Hayes.

398. For the same reasons discussed for claim 1[p], Hayes discloses that application control is performed on a network terminal. This could be any device on the terminal, including a device to be used by an end user. (Hayes, [0011] (disclosing that “[t]he system allows users to roam, that is, to log-in from any computer in the system at any time and have it configured automatically at run time according to the preferences stored for the user at the server”).) Hayes also provides for a “plurality of user stations, such as desktop personal computers **102**, mobile laptop computers **104**, workstations **106** (e.g., RISC computers), an administrator’s station **108** and a server **110**.” (*Id.*, [0037], Fig. 1.) Thus, Hayes discloses “**a device.**”

**(b) “a memory; and” (Claim 10[a])**

399. It is my opinion that Hayes renders obvious claim 10[a]. In the alternative, it is my opinion that claim 10[a] is obvious over Hayes in view of **Lambert** (EX1004; U.S. Patent App. Pub. 2002/0099952).

400. Hayes discloses that its system is implemented via a set of user stations connected to a network. (Hayes, [0015], [0013], [0037], Fig. 1.) Such user stations can include a desktop personal computer, a laptop computer, or other workstation. (*Id.*, Fig. 1, [0037].) A POSITA would have understood that any of these computers would have contained a “**memory**.” A “**memory**” is a fundamental part of any computer architecture, as shown in the following diagram of a “basic computer system” from a 1994 textbook:

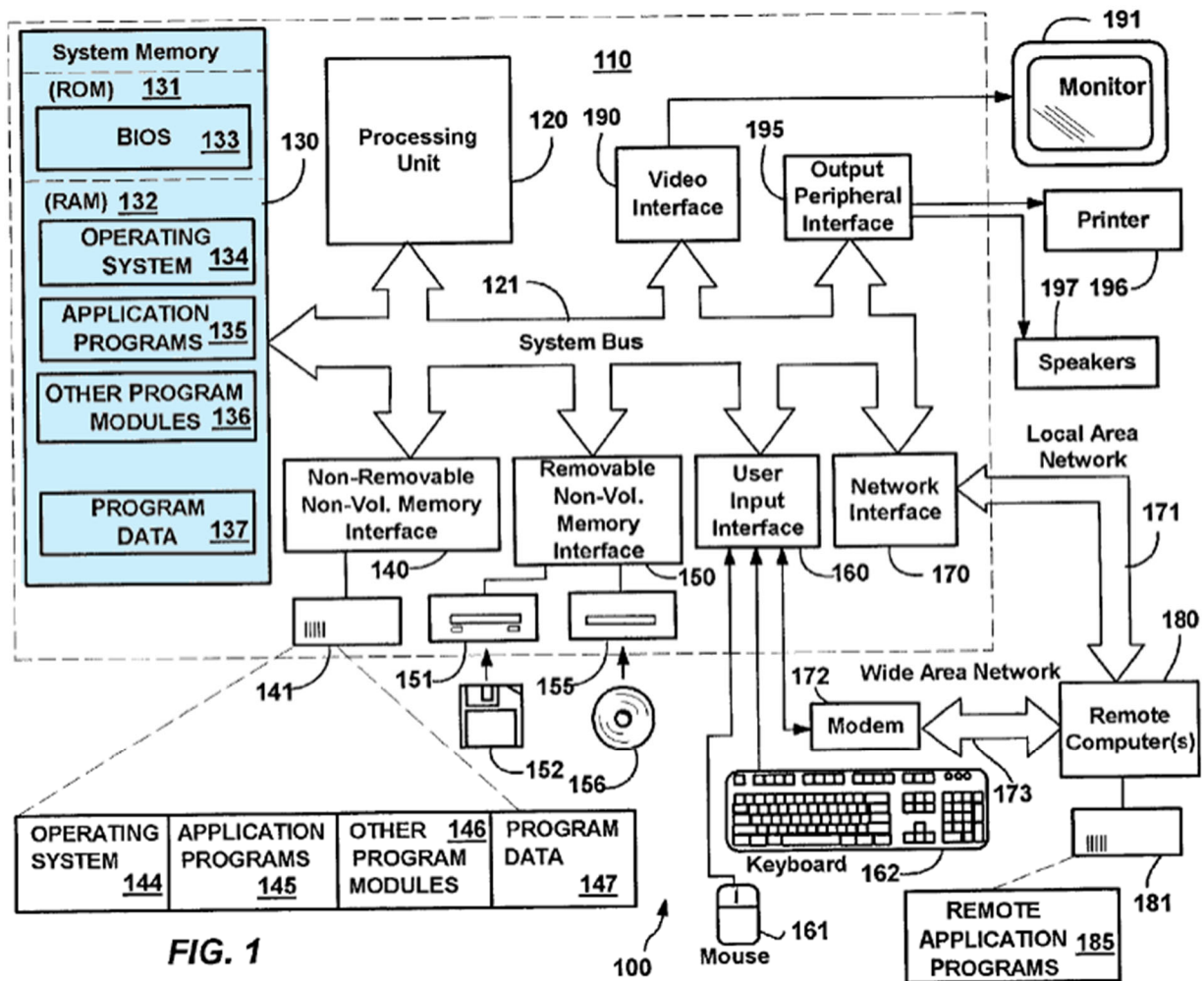


(EX1016 (K.F. Ibrahim, *Electronic Systems & Techniques* (1994)), p.008 (“The

program is stored in the memory unit.”.)

401. Further, it would have been obvious that any of Hayes’s computers contains a “**memory**” based on Lambert (EX1004; U.S. Patent App. Pub. 2002/0099952).

402. Lambert discloses the following architecture for a computer used with its system, including “system memory 131”:



(Lambert, Fig. 1 (highlighting added), [0031].) Lambert discloses that within system

memory **131**, “RAM **132** typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit **120**.” (*Id.*, [0031]; *see also id.* (disclosing that “basic input/output system **133** (BIOS), containing the basic routines that help to transfer information between elements within computer **110** ... is typically stored in ROM **131**”).)

403. **Motivation to Combine**: As I explained above, it would have been obvious for a POSITA to combine Hayes with Lambert. A POSITA would have looked to Lambert for implementation details of a computer in Hayes’s system. Specifically, a POSITA would have implemented Hayes’s system with user stations that contain a memory. Further, in the combined system, each of Hayes’s user stations would have a processor executing instructions stored in the memory, per Lambert’s disclosures. The application restriction functionality disclosed by Hayes would be implemented based on such instructions stored in the memory and executed by the processor.

404. Hayes and Lambert are analogous art in a similar field. Each relates to administration and management of a computer network to limit application use by users. (Hayes, [0001] (“the invention relates to server-based storage of software preferences (configuration data) for software retrieved from a server and executing at the desktop computer”); Lambert, [0078] (“an administrator (possibly multiple

administrators) constructs the various polices [sic] that make up the effective policy 502”), [0002] (“The present invention is generally directed to computer systems, and more particularly to an improved security framework for computer systems.”), [0080]-[0081], [0003].) Furthermore, each reference relates to administering the network of a business enterprise. (Hayes, [0001] (discussing invention as relating to computers “connected to a network such as a corporate intranet”), [0059] (discussing “enterprise modeling”), [0002]; Lambert, [0003] (discussing “enterprise computing environments” where “administrators begin to lose control over what software code the enterprise’s machines are executing”), [0007] (“In sum, in contemporary computer systems, running unknown code cannot be prevented, and indeed is necessary to an extent in many enterprises, yet doing so leads to increased support costs in system maintenance and helpdesk time, and decreased user productivity.”), *id.* (discussing the “rise in the usage of networks, email and the Internet for business computing”).)

405. A POSITA would have looked to Lambert for implementation details on the computer hardware to be used with Hayes’s system. Hayes does not focus on the hardware details of the computers involved in its system. Lambert provides such details, including the computer architecture shown in Figure 1 and the accompanying specification disclosures. (Lambert, [0029]-[0035].) Accordingly, a POSITA would

have looked to Lambert for implementation details on Hayes's system.

406. A POSITA would have had more than a reasonable expectation of success and could have implemented the proposed combination using conventional techniques without undue experimentation. The Hayes and Lambert combination is fundamental computing technology, as confirmed by the Ibrahim textbook from 1994. (EX1016 (K.F. Ibrahim, *Electronic Systems & Techniques* (1994), p.008 ("The program is stored in the memory unit."), Fig. 12.1) The proposed combination would have involved nothing more than the routine implementation of known techniques.

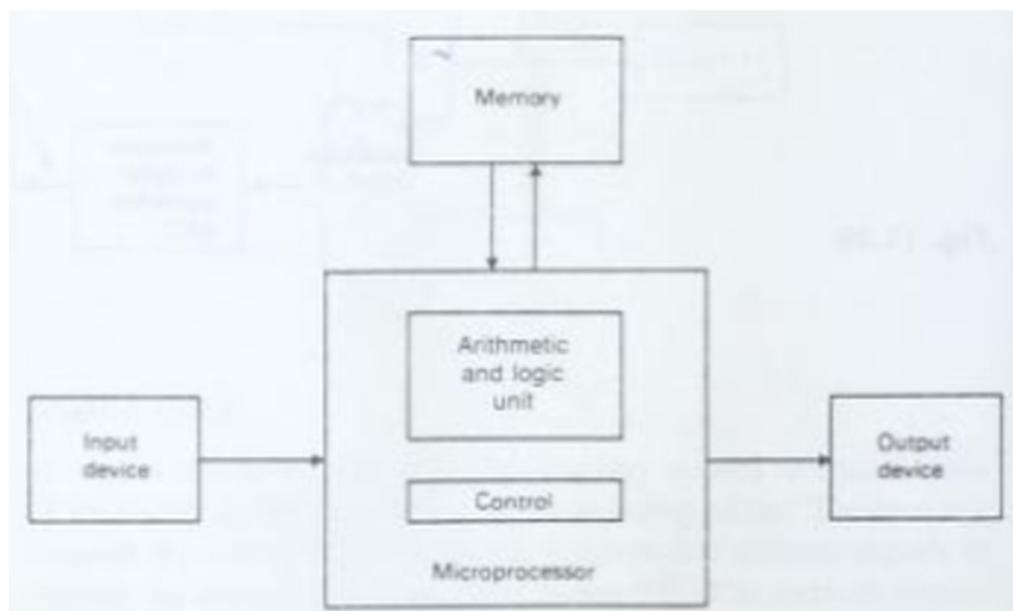
407. Hayes and Lambert are analogous art to the '571 patent for the same reasons described above.

(c) **“a processor coupled with the memory and configured by instructions stored in the memory to:” (Claim 10[b])**

408. It is my opinion that Hayes renders claim 10[b] obvious. In the alternative, it is my opinion that claim 10[b] is obvious over Hayes in view of **Lambert** (EX1004; U.S. Patent App. Pub. 2002/0099952).

409. Hayes discloses that its system is implemented via a set of user stations connected to a network. (Hayes, [0015], [0013], [0037], Fig. 1.) Such user stations can include a desktop personal computer, a laptop computer, or other workstation.

(*Id.*, Fig. 1, [0037].) A POSITA would have understood that any of these computers would have contained a “**processor coupled with the memory and configured by instructions stored in the memory.**” A “**processor coupled with the memory and configured by instructions stored in the memory**” is a fundamental part of any computer architecture, as shown in the following diagram of a “basic computer system” from a 1994 textbook:



(EX1016 (K.F. Ibrahim, *Electronic Systems & Techniques* (1994)), p.008.) As the above diagram shows, the microprocessor is coupled to the memory. (*Id.* (“Communication between the microprocessor and the memory, therefore, may take place in both directions, as shown.”).) The textbook further discloses that:

The microprocessor may carry out mathematical operations such as addition and multiplication, logical operations such as AND, OR, NOR

etc., or data transfer as instructed by a program. The program is a series of instructions which sets out the operations to be carried out step-by-step. The program is stored in the memory unit.

(*Id.* (emphasis added).)

410. As discussed above, claim 10[b] would further have been obvious over Hayes in view of **Lambert** (EX1004; U.S. Patent App. Pub. 2002/0099952). As I explained above, it would have been obvious for a POSITA to combine Hayes with Lambert. A POSITA would have looked to Lambert for implementation details of a computer in Hayes's system. Specifically, a POSITA would have implemented Hayes's system with user stations that contain a memory. Further, in the combined system, each of Hayes's user stations would have a processor executing instructions stored in the memory, per Lambert's disclosures. The application restriction functionality disclosed by Hayes would be implemented based on such instructions stored in the memory and executed by the processor.

**(d) “receive owner information from an owner of the device;” (Claim 10[b][i])**

411. As discussed above for claim 1[a], it is my opinion that claim 10[b][i] is disclosed by or would have been obvious based on Hayes and/or Hayes in light of Sprigg and Frank.

**(e) “receive owner control information that comprises:”  
(Claim 10[b][ii])**

412. As discussed above for claim 1[b], it is my opinion that claim 10[b][ii] is disclosed by or would have been obvious based on Hayes and/or in view of Hayes and Guedalia.

**(f) “a list of applications permitted for installation on the device, and” (Claim 10[b][ii][A])**

413. As discussed above for claim 1[b] and 1[b][i], it is my opinion that claim 10[b][ii][A] is disclosed by or would have been obvious based on Hayes and/or in view of Hayes and Guedalia.

**(g) “permissions associated with each permitted application in the list of applications;” (Claim 10[b][ii][B])**

414. As discussed above for claim 1[b][ii], it is my opinion that claim 10[b][ii][B] is obvious over Hayes in light of Sprigg.

**(h) “store the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information” (Claim 10[b][iii])**

415. As discussed above for claim 1[c], it is my opinion that claim 10[b][iii] is disclosed by or would have been obvious based on Hayes.

- (i) **“receive, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 10[b][iv])**

416. As discussed above for claim 1[d], it is my opinion that claim 10[b][iv] is obvious over Hayes in light of Sprigg.

- (j) **“determine whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 10[b][v])**

417. As discussed above for claim 1[e], it is my opinion that claim 10[b][v] is obvious over Hayes in light of Sprigg.

- (k) **“control application access to the local memory based upon the determining.” (Claim 10[b][vi])**

418. As discussed above for claim 1[f], it is my opinion that claim 10[b][vi] is obvious over Hayes in light of Sprigg.

## **11. Dependent claim 11**

419. For reference, claim 11 recites:

11. The device of claim 10, wherein the request to access the local memory comprises a request to erase data from the local memory.

(’571, 30:29-31 (Claim 11).)

420. For purposes of my analysis, claim 11 is substantially the same as claim 2. Therefore, for the reasons discussed above for claim 2, it is my opinion that

claim 11 is obvious over Hayes in light of Sprigg and over Hayes in light of Sprigg and Lambert (as discussed above for claim 10). Claim 11 is satisfied by Grounds 3, 4, and 5.

**12. Dependent claim 12**

421. For reference, claim 12 recites:

12. The device of claim 10, wherein the request to access the local memory comprises a request to read data from the local memory.

(’571, 30:32-34 (Claim 12).)

422. For purposes of my analysis, claim 12 is substantially the same as claim 3. Therefore, for the reasons discussed above for claim 3, it is my opinion that claim 12 is obvious over Hayes in light of Sprigg and over Hayes in light of Sprigg and Lambert (as discussed above for claim 10). Claim 12 is satisfied by Grounds 3, 4, and 5.

**13. Dependent claim 13**

423. For reference, claim 13 recites:

13. The device of claim 10, wherein the processor is further configured to restrict modification of the owner control information after the owner control information has been stored on the electronic device.

(’571, 30:35-38 (Claim 13).)

424. Claim 13 is satisfied by Grounds 3, 4, and 5.

425. It would have been obvious to a POSITA to implement the combination of Hayes and Sprigg such that **“the processor is further configured to restrict modification of the owner control information after the owner control information has been stored on the electronic device,”** for the same reasons as discussed for claim 4. For example, it would have been obvious to a POSITA that after a user terminal receives application permission information like Sprigg discloses, a user would be restricted from modifying that information.

426. For example, Sprigg discloses that one of the goals of its system is “protecting the resources of a device and the connected network,” due, for example, to the threat of damage caused by an application on a device or the network. (Sprigg, 1:45-52 (“This damage may be intended via a virus on the application or may be unintended where the application executes with poorly written code that unintentionally dominates a resource and makes it unavailable or damaged to other applications.”).) Accordingly, Sprigg discloses that its system checks whether permission information was modified before executing an application being checked against the permission information. (*Id.*, Fig. 4, 4:33-37, 5:25-38, 6:22-33, 6:51-7:23.) If it is determined that the permission information was modified (for example, on the basis of a digital signature), then Sprigg discloses preventing the application

from executing. (*Id.*)

427. It would have been obvious to implement such functionality in the Hayes-Sprigg combination. Thus, in the combined system, “**the processor is further configured to restrict modification** [*i.e.*, prevent modification without consequences to the execution of applications] **of the owner control information after the owner control information has been stored on the electronic device.**” Further, claim 13 would have been obvious over the combination between Hayes, Sprigg, and Lambert (as discussed above for claim 10).

#### **14. Dependent claim 14**

428. For reference, claim 14 recites:

14. The device of claim 10, wherein the owner control information includes an authorization record and an application identifier for each of the applications, and wherein the owner control information is provided by an external source through a wireless communication channel.

(’571, 30:39-43 (Claim 14).)

429. For purposes of my analysis, claim 14 is substantially the same as claim 5. Therefore, for the reasons discussed above for claim 5, it is my opinion that claim 14 is obvious over Hayes in light of Sprigg and over Hayes in light of Sprigg and Lambert (as discussed above for claim 10). Claim 14 is satisfied by Grounds 3,

4, and 5.

**15. Dependent claim 15**

430. For reference, claim 15 recites:

15. The device of claim 14, wherein the authorization record related to determining whether access to the local memory is allowed is provided by an external computer that is used to enforce policies for operating electronic devices within an organization.

(’571, 30:44-48 (Claim 15).)

431. For purposes of my analysis, claim 15 is substantially the same as claim 6. Therefore, for the reasons discussed above for claim 6, it is my opinion that claim 15 is obvious over Hayes in light of Sprigg and Hayes in light of Sprigg and Lambert (as discussed above for claim 10). Claim 15 is satisfied by Grounds 3, 4, and 5.

**16. Dependent claim 16**

432. For reference, claim 16 recites:

16. The device of claim 10, wherein an update to the owner control information is provided by an external source for storage on the electronic device.

(’571, 30:49-51 (Claim 16).)

433. For purposes of my analysis, claim 16 is substantially the same as claim 7. Therefore, for the reasons discussed above for claim 7, it is my opinion that

claim 16 is disclosed by Hayes and would have been obvious over Hayes in light of Sprigg and Lambert (as discussed above for claim 10). Claim 16 is satisfied by Grounds 3, 4, and 5.

**17. Independent claim 17**

**(a) “A non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the operations of:” (Claim 17[p])**

434. To the extent the preamble to claim 17 is limiting, it is my opinion that it is rendered obvious by Hayes. In the alternative, it is my opinion that the preamble to claim 17 is obvious over Hayes in light of Lambert (EX1004; U.S. Patent App. Pub. 2002/0099952).

435. Hayes discloses that its system is implemented via a set of user stations connected to a network. (Hayes, [0015], [0013], [0037], Fig. 1.) Such user stations can include a desktop personal computer, a laptop computer, or other workstation. (*Id.*, Fig. 1, [0037].) A POSITA would have understood that any of these computers would have contained a **“non-transitory computer-readable medium with instructions stored thereon, wherein the instructions are executable by a processor to cause the processor to perform the [claimed] operations[.]”** A **“non-transitory computer-readable medium with instructions stored thereon”** and **“a processor”** to execute those instructions are a fundamental part of any

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

computer architecture, as shown in the above reproduced diagram of a “basic computer system” from a 1994 textbook. (EX1016 (K.F. Ibrahim, *Electronic Systems & Techniques* (1994)), p.008.) The textbook discloses that:

The microprocessor may carry out mathematical operations such as addition and multiplication, logical operations such as AND, OR, NOR etc., or data transfer as instructed by a program. The program is a series of instructions which sets out the operations to be carried out step-by-step. The program is stored in the memory unit.

(*Id.* (emphasis added).)

436. As discussed above in claim 10[b], the preamble to claim 17 would further have been obvious over Hayes in view of **Lambert** (EX1004; U.S. Patent App. Pub. 2002/0099952). For example, Lambert discloses that it can be implemented on a computer including “computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 131 and random access memory (RAM) **132**. (Lambert, [0031] (emphasis added); *see also id.* (disclosing that “basic input/output system **133** (BIOS), containing the basic routines that help to transfer information between elements within computer **110** ... is typically stored in ROM **131**”).) As I explained above, it would have been obvious for a POSITA to combine Hayes with Lambert. A POSITA would have looked to Lambert for implementation details of a computer in Hayes’s system. Specifically,

a POSITA would have implemented Hayes's system with user stations that contain a memory—*i.e.*, a **“non-transitory computer-readable medium with instructions stored thereon.”** Further, in the combined system, each of Hayes's user stations would have a processor executing instructions stored in the memory, per Lambert's disclosures. The application restriction functionality disclosed by Hayes would be implemented based on such instructions stored in the memory and executed by the processor.

**(b) “receiving owner information from an owner of an electronic device;” (Claim 17[a])**

437. For purposes of my analysis, claim 17[a] is substantially the same as claim 1[a]. Therefore, for the reasons discussed above for claim 1[a], it is my opinion that claim 17[a] is disclosed by or would have been obvious based on Hayes and/or Hayes in light of Sprigg and Frank.

**(c) “receiving owner control information that comprises:” (Claim 17[b])**

438. For purposes of my analysis, claim 17[b] is substantially the same as claim 1[b]. Therefore, for the reasons discussed above for claim 1[b], it is my opinion that claim 17[b] is disclosed by or would have been obvious based on Hayes and/or Hayes in light of Sprigg and Frank.

**(d) “a list of applications permitted for installation on the device, and” (Claim 17[b][i])**

439. For purposes of my analysis, claim 17[b][i] is substantially the same as claim 1[b][i]. Therefore, for the reasons discussed above for claims 1[b] and 1[b][i], it is my opinion that claim 17[b][i] is disclosed by or would have been obvious based on Hayes and/or Hayes in light of Sprigg and Frank.

**(e) “permissions associated with each permitted application in the list of applications;” (Claim 17[b][ii])**

440. For purposes of my analysis, claim 17[b][ii] is substantially the same as claim 1[b][ii]. Therefore, for the reasons discussed above for claim 1[b][ii], it is my opinion that claim 17[b][ii] is obvious over Hayes in light of Sprigg.

**(f) “storing the owner control information in a protected data store to prevent alteration or deletion of the owner control information in response to authenticating the owner control information using the owner information;” (Claim 17[c])**

441. For purposes of my analysis, claim 17[c] is substantially the same as claim 1[c]. Therefore, for the reasons discussed above for claim 1[c], it is my opinion that claim 17[c] is disclosed by or would have been obvious based on Hayes.

**(g) “receiving, from an application operating on the electronic device, a request to access local memory on the electronic device;” (Claim 17[d])**

442. For purposes of my analysis, claim 17[d] is substantially the same as claim 1[d]. Therefore, for the reasons discussed above for claim 1[d], it is my

opinion that claim 17[d] is obvious over Hayes in light of Sprigg.

- (h) **“determining whether the application is allowed to access the local memory in response to identifying a permission associated with the application in the owner control information; and” (Claim 17[e])**

443. For purposes of my analysis, claim 17[e] is substantially the same as claim 1[e]. Therefore, for the reasons discussed above for claim 1[e], it is my opinion that claim 17[e] is obvious over Hayes in light of Sprigg.

- (i) **“controlling application access to the local memory based upon the determining.” (Claim 17[f])**

444. For purposes of my analysis, claim 17[f] is substantially the same as claim 1[f]. Therefore, for the reasons discussed above for claim 1[f], it is my opinion that claim 17[f] is obvious over Hayes in light of Sprigg.

## **18. Dependent claim 18**

445. For reference, claim 18 recites:

18. The non-transitory computer-readable medium of claim 17, wherein the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device.

(’571, 31:10-13 (Claim 18).)

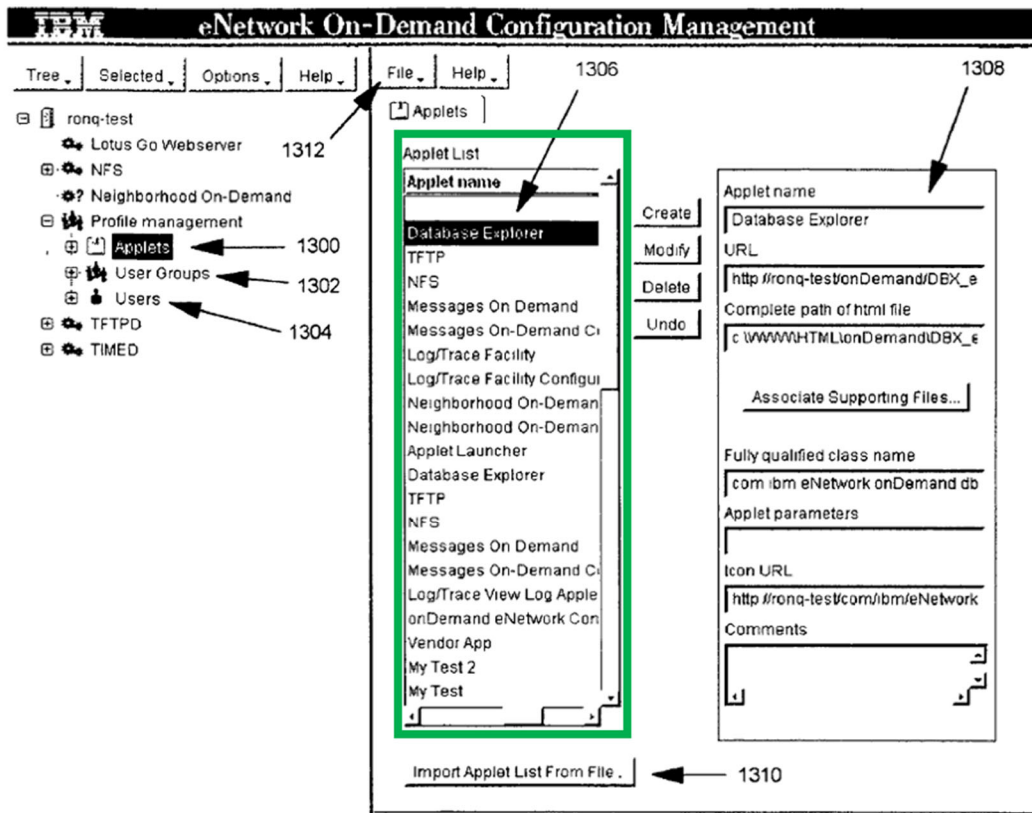
446. As discussed above for claims 8[p], 1[b][ii], and 5, it is my opinion that claim 18 would have been obvious over Hayes in light of Sprigg and Hayes in light

of Sprigg and Lambert (as discussed above for claim 17). Claim 18 is satisfied by Grounds 3, 4, and 5.

447. The limitation **“the owner control information includes an authentication record and an identifier for each application allowed to be executed on the electronic device”** would have been obvious over Hayes in view of **Sprigg** (EX1012; U.S. Patent No. 7,743,407). As I explained above, Hayes discloses an interface via which a network administrator can determine whether applications are allowed for different users on an application by application basis. For example, in Figure 13, Hayes shows an “Applet List” with options for an administrator to “Create” or “Delete” applets:

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

Fig. 13



(Hayes, Fig. 13 (highlighting added), [0085].) Further, Hayes discloses a screenshot of an interface where an administrator can allow a subset of permitted applications for a particular user (Figure 24), or for groups of users (Figure 17):

Fig. 24

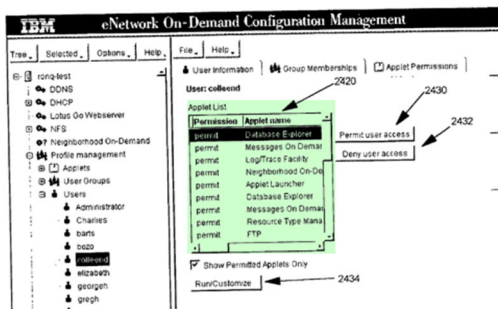
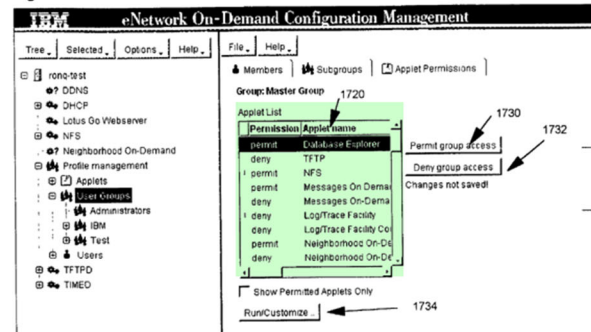


Fig. 17



(*Id.*, Figs. 24 & 17 (highlighting added), [0093], [0088].)

448. Further, Hayes teaches that when an end user brings up the desktop on a terminal, the “desktop objects calls a method ... to get a list of the software to which the user has access permission.” (Hayes, [0071] (emphasis added).)

449. Hayes discloses that the server provides “a user friendly name, the applet’s URL, the URL of an icon for the applet, etc. (information that is required for the desktop to represent the applet on the desktop and to load and launch it.)” (Hayes, [0071] (emphasis added).)

450. Moreover, “the server stores a plurality of user applications for downloading to user stations and further stores access permissions for the applications.” (Hayes, [0013]) (emphasis added).) Hayes explains that the server uses a user’s identifying information to “build a list of applications for which the user has access permission.” (*Id.*) The server further “downloads to the station a list of applications to which the user has access permission,” and “[t]he user station uses the list to build a folder containing only the applications from the list to which the user has access permission.” (*Id.*; *see also id.*, claim 1 (reciting “downloading to the station the list of applications for which the user has access permissions” and requesting “a download of the corresponding application to the user station”).)

451. Thus, Hayes alone discloses that “**the owner control information**

**includes ... an identifier for each application allowed to be executed on the electronic device.”**

452. Further, as I explained above, Sprigg discloses a computer network where a wireless device **300** contains “applications **310** each with a permission list **320.**” (Sprigg, 5:41-43.) Sprigg discloses that “each application [**310**]<sup>7</sup> may have a separate permission list associated with that application[.]” (*Id.*, 5:45-48.) Sprigg further discloses that these permissions associated with each application “contain[] a listing of the resources **315** and an indication whether the application has permission to access any of the specific resources **315** on the device.” (*Id.*, 5:63-66.) For example, Sprigg discloses that the permission lists can control access to “memory, including primary and secondary storage” and “files stored in memory, including the read, write and modify operations on such files.” (*Id.*, 4:14-21.) Thus, Sprigg discloses that “**the owner control information includes an authentication record.**” Considering Sprigg’s permission lists to include “**an authentication record**” is consistent with the ’571 patent specification. (’571, 7:46-53 (“the each application authentication records includes a field that designates the application appropriately (e.g., allowed, required, excluded, etc.) and can include a field

---

<sup>7</sup> See footnote 6.

containing an application identifier.”).)

453. As I also explained above, it would have been obvious to modify Hayes’s administrator interface program (shown in, *e.g.*, Hayes’s Figs. 13, 17, and 24) in light of Sprigg to allow an administrator to provide application resource restrictions on an application-by-application basis. This would have led to the server providing a client device **“owner control information”** including **“an authentication record and an identifier for each application allowed to be executed on the electronic device.”**

454. For example, Hayes discloses that a user terminal receives from the server a “list of the software to which the user has access permission” including “a user friendly name, the applet’s URL, the URL of an icon for the applet, etc. (information that is required for the desktop to represent the applet on the desktop and to load and launch it).” (Hayes, [0071] (emphasis added).) This information includes various **“identifier[s]”**—including the name and URL of the applet. (*Id.*; *see also* Sprigg, 5:25-28 (“The application, in one embodiment, has a unique identifier to distinguish it from other applications.”), Fig. 3.) Further, in the combination of Hayes and Sprigg, the **“identifier”** information would be paired with an **“authentication record”**—*e.g.*, the resource access restriction information disclosed by Sprigg. (*Id.*, 5:41-43, 5:45-48, 5:63-66.)

**19. Dependent claim 19**

455. For reference, claim 19 recites:

19. The non-transitory computer-readable medium of claim 17, wherein the request to access the local memory comprises a request to erase data from the local memory.

(’571, 31:14-16 (Claim 19).)

456. For purposes of my analysis, claim 19 is substantially the same as claim 2. Therefore, for the reasons discussed above for claim 2, it is my opinion that claim 19 is obvious over Hayes in light of Sprigg and Hayes in light of Sprigg and Lambert (as discussed above for claim 17). Claim 19 is satisfied by Grounds 3, 4, and 5.

**20. Dependent claim 20**

457. For reference, claim 20 recites:

20. The non-transitory computer-readable medium of claim 17, wherein the request to access the local memory comprises a request to read data from the local memory.

(’571, 31:17-19 (Claim 20).)

458. For purposes of my analysis, claim 20 is substantially the same as claim 3. Therefore, for the reasons discussed above for claim 3, it is my opinion that claim 20 is obvious over Hayes in light of Sprigg and Hayes in light of Sprigg and Lambert (as discussed above for claim 17). Claim 20 is satisfied by Grounds 3,

4, and 5.

## **VI. NO SECONDARY CONSIDERATIONS OF NONOBVIOUSNESS**

459. I am not aware of any evidence suggesting that the claims are not obvious, such as the following secondary considerations: commercial success, unexplained results, long felt but unsolved need, industry acclaim, simultaneous invention, copying, skepticism by experts, and failure of others.

460. I understand from counsel that PO has not identified any secondary considerations evidence. Furthermore, as explained in Part III.B, I understand that “secondary considerations” may be used as indicia of nonobviousness provided that there is a nexus to the invention claimed. To the extent PO later provides information, I reserve the right to supplement my analysis and opinions.

## **VII. CONCLUSION**

461. In signing this Declaration, I recognize that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in this proceeding. If required, I will appear for cross-examination at the appropriate time. I reserve the right to offer opinions relevant to the invalidity of the challenged claims at issue and/or offer testimony in support of this Declaration.

Declaration of Nathaniel Polish, Ph.D. in Support of  
Petition for *Inter Partes* Review of  
U.S. Patent No. 9,542,571 B2

I hereby declare that all statements made herein of my own knowledge are true and that all statements are made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.

Dated: October 8, 2025

Respectfully submitted,



---

Nathaniel Polish

# APPENDIX A

**NATHANIEL POLISH, Ph.D.**  
**Daedalus Technology Group, Inc.**  
 350 Seventh Avenue  
 New York, NY 10001  
 (212) 684-3890

**business experience**

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>2019-present</b>    | <b>President, Founder</b><br><b>SuperAlert, Inc.</b><br>SuperAlert has developed a range of wireless sensors used for monitoring building systems in large New York City residential buildings. SuperAlert manufactures, deploys, and operates sensor suites and generates notifications and alerts for building personnel and owners.                                                                                                                                                                                                | <b>NEW YORK, NY</b>   |
| <b>1980-present</b>    | <b>President</b><br><b>Daedalus Technology Group, Inc. Successor to NPS ASSOCIATES</b><br>Co-founded computer consulting firm. Employs up to twenty people as needed.                                                                                                                                                                                                                                                                                                                                                                 | <b>NEW YORK, NY</b>   |
| <b>clients include</b> | Intellectual Property Consulting. Various anonymous clients.<br><b>Consulting on patent valuation and strategy:</b> Act as an advisor on technical and intellectual property matters to various clients. Developed intellectual property for various companies. 2001- present.                                                                                                                                                                                                                                                        | <b>NEW YORK, NY</b>   |
|                        | SpokenHub.<br><b>Predictive dialer deployment and operation:</b> During the 2012 election cycle assembled and ran a team of engineers to deploy, debug, and operate a large scale outbound calling server farm. This server farm supported hundreds of agents and millions of minutes of calling. 2012.                                                                                                                                                                                                                               | <b>NEW YORK, NY</b>   |
|                        | Risk Solutions International.<br><b>Risk management:</b> Developed technology platform to allow for complex question and answer sessions with airport managers. The results of the sessions then generated planning documents used in risk management. Results were published as part of a Transportation Research Board research program. 2011-2013.                                                                                                                                                                                 | <b>NEW YORK, NY</b>   |
|                        | Smart Systems/Specialty Acquirer.<br><b>Advanced Transit fare collection:</b> Founding member of board of directors. Advisor on technical and intellectual property matters. Developed intellectual property for the company. The company is engaged in the development and sale of advanced fare collection systems for mass transit using RFID technologies. 2004-present.                                                                                                                                                          | <b>NEW YORK, NY</b>   |
|                        | Skywi.<br><b>Wireless broadband:</b> Founding board of directors member. Advisor on technical and intellectual property matters. The company provides a variety of wireless broadband services to semi-rural customers using mesh networks. 2004-2009                                                                                                                                                                                                                                                                                 | <b>FORT WORTH, TX</b> |
|                        | Placecorp.<br><b>Wireless text messaging system:</b> Designed and developed a very large scale, multi-platform text messaging system. Acted as the lead technologist for a startup. In this capacity attended many venture capital meetings and developed all technical sections to the business plans. The system integrated advanced Interactive Voice Response (IVR) with email, paging, and SMS messaging. Oversaw and planned initial development of very small paging device to be manufactured in very high volume. 2000-2001. | <b>NEW YORK, NY</b>   |
|                        | Marketboy.<br><b>Distributed market making system:</b> Provided a range of services in the areas of product definition, specification, and implementation strategy. Marketboy was a distributed system that allowed prospective purchasers and vendors to make bids and ask offers for proposed transactions. 2000.                                                                                                                                                                                                                   | <b>NEW YORK, NY</b>   |
|                        | Savos.<br><b>Telephone to streaming audio bridge:</b> Developed, designed and deployed an industrial strength IVR system that allows users to access streaming media via their cell phones. The system supports up to 96 streams on a single chassis. Developed web based content management system and interface for customizable user preferences. 2000.                                                                                                                                                                            | <b>NEW YORK, NY</b>   |

deliverENow.

NEW YORK, NY

**Online delivery system:** Developed a proof of concept prototype of online delivery system. This consisted of a stock clerk server written for Windows CE (Clio) with a CDPD network connection. It demonstrated how purchase and delivery information would be sent to an in-store stock person who prepares them for pickup by a member of the deliverENow courier network. Provided strategic technical advice. Served on board of advisors. Wrote technical specification of business and logistical components of the system. 2000.

Togglethis.

NEW YORK, NY

**Animation distribution system:** Developed critical components of initial version of email-delivered animation system. Components included MacroMedia Director Xtras as well as encryption functions. Developed tools to distribute and manage Togglethis's content, DTG built a custom UNIX email list-server. This server allowed Toggle administrators to create groups, upload episodes, and schedule the delivery of their content. Developed system architecture and language specification for the next version of the IC Engine, which drives the characters. 1998-1999.

JuniorNet.

BOSTON, MA

**Children's on-line service:** Designed, developed and lead the implementation of a large scale network system for delivery of children's entertainment and education content. Worked with the president and other key players to fit a technology strategy to corporate goals. System is required to serve from 200,000 to 1,000,000 subscribers and be supportable over three to five years. All project goals met within a \$1,000,000+ budget. 1997-2000.

One Click Charge.

NEW YORK, NY

Provide a wide range of consulting services starting with technology evaluation for the principal investor. Provided services in the areas of product definition, team formation and implementation strategy. Developed significant components of a substantial Internet micropayment and authentication system. 1998-2000.

Swatch.

WEEHAWKEN, NJ

**Ticketing system:** Implemented a radio frequency identification (RFID) based system for providing access to the 1998 Goodwill Games utilizing RFID tagged wristwatches. 1998-1999.

Instant Video Technologies, Inc./Burst.com

SAN FRANCISCO, CA

**Burstware:** Designed and developed a series of products to deliver digital video and audio materials over wide-area internet using consumer grade computers. Products were designed to fit within the client's existing patent portfolio. 1995-1997.

**Technical evaluation:** Provided technology strategy and evaluation services and acted as Technology Director. 1995-1997.

Assurenent.

BETHESDA, MD

**Internet Insurance system:** Designed and developed a system for utilization of the Internet for the distribution and control of insurance agent support software. System can handle tens of thousands of simultaneous users. Member of Board of Directors. 1995-2002.

New Zealand Antarctic Project (NZAP) and US Antarctic Program (USAP).

ANTARCTICA

**Penguin Weighbridge:** Designed, developed, and deployed system for tracking the comings and goings, weights, and Ids of Adelie penguins in their natural environment on three colonies on Ross Island, Antarctica. Systems run continuously for months in adverse conditions. System was upgraded and replaced in 2016. 1994-present.

Electronic Digital Documents, Inc.

NEW YORK, NY

**Check Image Compression system:** 1995-1999.

American Veterinary Identification Devices, Inc.

NORCO, CA

**AVID reader:** Designed and developed digital computer components of radio frequency identification system. Work involved imbedded microcontrollers and real-time digital signal processing in very noisy environment. Designed communications protocols including encryption and error checking schemes. Product in high volume (50,000 unit) production. 1988-1995.

Amprobe Instrument, Inc.

LONG ISLAND, NY

**REMCON tester:** Designed and implemented product life-cycle test fixture for a new and innovative solid state switch. Test fixture used by Underwriters Labs for approval. 1988.

Personal Computer Card Corporation

NEW YORK, NY

**Smart Cards:** Designed smart card reader/writer system. Performed general design and component selection and wrote software for smart card communications. System design implemented in commercial product. 1987.

The Dun & Bradstreet Corporation

NEW YORK, NY

**Voice editing systems:** Designed and built all parts of four generations of interactive voice editing systems. Editing systems produce output used in extensive, high quality speech synthesis system that is part of larger information delivery system. The systems are built on networks of computers in a variety of programming languages and systems. The system involved interactive user interfaces, screen windows, signal processing, and voice file systems. 1982-1991.

1997-2001

### **Co-Founder, Director and CTO**

**I-RECALL, INC.**

NEW YORK, NY

Co-founded a company that developed software to enable note-taking and linking of notes to streaming media. Used platforms such as PalmPilot and CrossPad for note-taking and provided time-stamped links to audio and video media. Company sold to a focus group company.

1996-1999

### **Co-Founder, Director, CTO & Principal Product Designer**

**SOLILOQUY, INC.**

NEW YORK, NY

**Natural language interfaces to databases:** Co-founded in 1996 a company to provide next generation interfaces to structured databases. Developed prototype system using speech recognition and speech synthesis to provide access to music and ecommerce databases. Raised \$1.5 million in angel investments. Company has raised a total of \$8 million through a variety of institutional and individual investors. Hired replacement CTO and exited company in 1999.

1991-1992

### **President & Principal Product Designer**

**SIMPLICITY COMPUTING, INC.**

NEW YORK, NY

Co-founded in 1991 a computer peripherals manufacturing company concentrating on portable products with international mass-market appeal. Main product: Simplicity Portable Drive, an IBMPC parallel port connected, portable disk storage system. Marketed domestically and in 25+ countries. Products marketed direct via telemarketers, trade shows, sales reps, and national advertising. Products distributed through dealers, distributors and national catalog houses. Company employed 10 people.

- Wrote business plan and raised \$350,000 startup funding
- Established marketing plans
- Directed marketing of products in trade shows, national advertisements and focus groups
- Managed employees
- Designed hardware and software for products
- Supervised hardware & software implementation teams
- First units shipped less than six months from start of project
- Supervised all aspects of manufacturing and testing process
- Contracted with four manufacturing facilities and many suppliers for production
- Supervised and established call-in customer support services

1989-1999

### **President & CEO**

**MEASUREMENT & CONTROL PRODUCTS, INC.**

NEW YORK, NY

Founded in August 1989 an electronic products development company. M&CP designs, develops, markets and sells its own products through retail, wholesale and catalog channels domestically and abroad. All manufacturing is contracted. Company was profitable in its first year of operation.

**Flagship product:**

**BitView:** Hand held RS-232 data communications diagnostic monitor. Invented, developed and produced hardware and software. Developed and oversaw implementation of marketing strategies, budgets, and business plans. Product currently in third production run.

**education**

1980-1993

**COLUMBIA UNIVERSITY**

NEW YORK, NY

Ph.D. in Computer Science, May 1993.

Thesis: *Mixed Distance Measures for the Optimization of Concatenative Vocabularies in Speech Synthesis.*

MPhil in Computer Science, December 1989.

MS in Computer Science, December 1987.

BA in Physics, Columbia College, May 1984.

**teaching positions**

1997

**COLUMBIA UNIVERSITY**

NEW YORK, NY

Adjunct Professor, Computer Science.

Advanced undergraduate course: Artificial Intelligence.

1989

**COLUMBIA UNIVERSITY**

NEW YORK, NY

Graduate Lecturer, Computer Science.

Advanced undergraduate course: Software Design. Taught 68 advanced undergraduates. Supervised two teaching assistants.

Students implemented full spreadsheet application under UNIX.

1984-1985

**CITY UNIVERSITY OF NEW YORK**

NEW YORK, NY

Adjunct Professor, Experimental Psychology.

Graduate-level course: Computer Methods in Experimental Psychology.

**publications and patents**

2024

Beth Polish, Nathaniel Polish, Seth Godin, and Robert Gehorsam. Real-time event and participant communication systems. United States Patent 11,962,628. April 16, 2024.

2022

Nathaniel Polish. Calibration apparatus and method. United States Patent 11,215,499. January 4, 2022.

2016

Michael L. Beigel, Nathaniel Polish, Steven R. Frank, and Robert E. Malm. Electronic identification system with improved sensitivity. United States Patent 9,430,728. August 30, 2016.

2010

Michael L. Beigel, Nathaniel Polish, Steven R. Frank, and Robert E. Malm. Electronic Identification System with Improved Sensitivity. United States Patent 7,737,821B2. June 15, 2010.

2009

Martin Silbernagl and Nathaniel Polish. Learning Fare Collection System for Mass Transit. United States Patent 7,568,617. August 4, 2009.

2009

Martin Silbernagl and Nathaniel Polish. Learning Fare Collection System for Mass Transit. United States Patent 7,566,003. July 28, 2009.

2009

Michael L. Beigel, Nathaniel Polish, Steven R. Frank, and Robert E. Malm. Electronic identification system with improved sensitivity. United States Patent 6,472,975. October 29, 2002.

2002

Nathaniel Polish. Bilateral speech system. Speech dialogs for database access. United States Patent 6,430,531. August 6, 2002.

1999

Nathaniel Polish. System and method for distributing and managing digital video information in a video distribution network. United States Patent 5,963,202. October 5, 1999.

1993

Michael L. Beigel, Nathaniel Polish and Robert E. Malm. Multi-Mode Identification System. Fundamental RFID technology. United States Patent 5,235,326. August 10, 1993.

1991

Nathaniel Polish. Mixed Distance Measures for Synthetic Speech Evaluation. In Proceedings of ICASSP-91, Toronto, Canada, 1991.

1988

Nathaniel Polish. A Distributed Signal Processing Facility for Speech Research. In Proceedings of AVIOS88, San Francisco, CA. October 4-6 1988.

1987

Nathaniel Polish. Mixed Distance Measures for Optimizing Concatenative Vocabularies for Speech Synthesis: A Thesis Proposal. Columbia University Department of Computer Science technical report number CUCS-310-87, 1987.

1983

M. Morris, N. Polish, B. Zuckerman, and N. Kaifu. The Temperature of Molecular Gas in the Galactic Center Region. The Astronomical Journal, 88(8):1228-1235, August 1983.

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>research interests</b>     | Computer Speech, Distributed Systems, Interactive Environments. Software Engineering, Systems Engineering, Technology Policy. Knowledge-Based Approaches to Signal Processing. Computational Physics, Non-Linear Dynamics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>professional societies</b> | International Society for Electrical and Electronics Engineers (IEEE), Association of Computing Machinery (ACM), American Association for the Advancement of Science (AAAS).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>other interests</b>        | Foreign Policy, Political Science, Long Distance Bicycling, United States Space Program.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>grants</b>                 | <ul style="list-style-type: none"> <li>• AT&amp;T Special Projects Grant of \$25,000 for synthetic speech, 1986.</li> <li>• Financial support for Ph.D. work was provided by the New York State Science and Technology Foundation Center for Advanced Technology in Computers and Information Systems at Columbia University.</li> <li>• Santa Fe Institute Complex Systems Summer School, 2003. Month-long workshop in agent-based models, non-linear systems, and complexity.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>1982-present</b>           | <p><b>Technology development projects</b></p> <p>Some technology development projects have included:</p> <p><b>Wildlife Tracking Systems:</b> Implemented a remote monitoring system to track and weigh Adelie penguins on Ross Island, Antarctica. System was debugged on-site and made to function in adverse environmental circumstances. 1994-1997, 2016.</p> <p><b>Internet Systems:</b> Implemented a LINUX Internet server with FTP and gopher services. Installed an Internet client for IBM/PC platform. 1994-1995.</p> <p><b>Image Compression Technology:</b> Developed proof-of-concept system for a system to compress images of checks to very small file size. 1994.</p> <p><b>Biomedical Systems:</b> Implemented a large biomedical system used in patient diagnostics. Provided all necessary materials for Food and Drug Administration compliance. 1992-1993.</p> <p><b>Synthetic Speech Systems:</b> Implemented and supported several generations of synthetic speech systems for commercial as well as research purposes. 1985-1999.</p> <p><b>Graphics:</b> Developed high-speed drivers for several graphical devices and evaluated their applicability for interactive uses. Devices included: Vectrix, RAMTEK, Apple Lisa, and IBM Enhanced Graphic Adapter. 1983-1987.</p> <p><b>Voice Boards:</b> Specified function requirements for several generations of high quality voice boards for Q-bus (PDP-11), Apple, MultiBus, and IBMPC bus. Developed high-speed drivers for each of the boards. 1982-1986.</p> <p><b>Video Disk and Touch Screens:</b> Developed experimental interactive system utilizing computer controlled video disks and touch screens. 1982.</p> |
| <b>1994-present</b>           | <p><b>Intellectual property projects</b></p> <p><b>A separate document detailing intellectual property projects is available on request.</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>tools</b>                  | <p>Languages commonly used:</p> <p>Pascal 1980-1988</p> <p>C 1985-present.</p> <p>Other languages used: C++, Lisp, Java and Python .</p> <p>Assembler:</p> <p>Intel 8048, 8051, 8088-pentium</p> <p>Motorola 680xx</p> <p>TI 320xx signal processors</p> <p>Zilog Z8, Z80, PIC</p> <p>Protocols include:</p> <p>TCP/IP, UDP, RPC and NFS</p> <p>Operating systems commonly used:</p> <p>UNIX, MSDOS, Windows and p-system.</p> <p>In circuit emulators.</p> <p>Database tools.</p> <p>ARM processors for embedded systems.</p> <p>I<sup>2</sup>C bus interfacing.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>contact information</b>    | <p>polish@dtgroup.com</p> <p>Office: (212) 684-3890</p> <p><b>Academic and business references available upon request.</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



Nathaniel Polish, Ph.D. ♦ Daedalus Technology Group, Inc. ♦ polish@dtgroup.com  
**Summary of Experience in Intellectual Property Matters, as of March 2025**

| Date              | Case and Jurisdiction                                                                                                                                                                                                                                                                                                | Work Product                                                                         | Counsel, Nature of Case and Additional Notes                                                                                                                                                                                                                                     |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 06/2024 - present | <i>Valerie Torres and Rhonda Hyman, individually and on behalf of all others similarly situated, v. Prudential Financial, Inc, Activeprospect, Inc., and Assurance IQ, LLC.</i><br>Case No. 3:22-cv-07465-CRB.<br>In The United States District Court For The Northern District of California San Francisco Division | Declarations; deposition.                                                            | Retained by Munger, Tolles & Ollson LLP (contact: Grace Davis-Fisher) representing Prudential. This is a class action related to alleged wire-tapping in connection with software to document user actions on a website. Case is ongoing.                                        |
| 07/2023 - 03/2025 | <b>Motorola Solutions, Inc. Petitioner</b> v. STA Group LLC. Case IPR2023-01295, US Patent 8,994,830 B2. United States Patent and Trademark Office.                                                                                                                                                                  | Declaration in support of invalidity in the context of an IPR, deposition.           | Retained by Baker Botts (contact: Katharine Burke) representing Motorola. This is an IPR related to a patent concerning mobile communications by emergency services. The IPR was instituted and the patent was found invalid.                                                    |
| 09/2022 - 05/2024 | <i>Staton Techiya, LLC and Synergy IP Corporation v. Samsung Electronics Co. LTD and Samsung Electronics America, Inc.</i><br>Case No. 2:21-CV-004130-JRG-RSP.<br>In The United States District For The Eastern District of Texas Marshall Division                                                                  | Expert reports on non-infringement and invalidity; depositions.                      | Retained by Kirkland and Ellis (contact: Alex Henriques) representing Samsung. This is a patent dispute related to intelligent wireless headsets, noise cancellation, and speech detection. Case resolved in our favor due to issues of "unclean hands".                         |
| 06/2022 - 07/2024 | <i>NantWorks, et al. v. Niantic</i><br>No. 20-cv-06262-LB<br>N.D. Cal.                                                                                                                                                                                                                                               | Expert reports; depositions.                                                         | Retained by Cooley (contact: Allie Leeper) representing Niantic. This is a patent case involving technology for augmented reality applications and games. I am working on non-infringement and invalidity. Case dismissed on summary judgement of invalidity on section 101.     |
| 02/2022 - 11/2023 | <b>VB Assets, LLC</b> v. <i>Amazon.com Inc. et al.</i><br>C.A. No. 1:19-cv-01410-MN<br>In the United States District Court for the District of Delaware                                                                                                                                                              | Expert reports on infringement and validity; depositions; <b>testimony at trial.</b> | Retained by Wilson Sonsini (contact: Ryan Smith and James Yoon) representing VB Assets, LLC. This is a patent case involving speech recognition and natural language processing in the Alexa system. I testified at trial. We prevailed at trial and the jury found willfulness. |
| 05/2021 - 06/2024 | <i>Linkable Networks, Inc. v. Mastercard Incorporated and Mastercard International Incorporated.</i> Index No.:651964/2019 in the Supreme Court of the State of New York County of New York                                                                                                                          | Expert reports; depositions; <b>testimony at trial.</b>                              | Retained by Baker Botts (contact: Jennifer Tempesta) representing Mastercard. This is a misappropriation of trade secrets case. I testified at trial. We prevailed.                                                                                                              |
| 06/2021 - 11/2021 | <i>USC IP Partnership, L.P. v. Facebook, Inc.</i><br>Civil Action No. 6:20-cv-00555-ADA<br>In The United States District Court for the Western District of Texas Waco Division                                                                                                                                       | Expert reports on infringement and invalidity; depositions.                          | Retained by Cooley (contact: Phillip E. Morton) representing Facebook. This is a patent dispute involving user interfaces and websites. This case was dismissed.                                                                                                                 |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                   |                                                                                                                                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 04/2019 - 07/2019 | <b>Samsung Electronics Co., LTD and Samsung Electronics America, Inc., Petitioners v. SpeakWare, Inc.</b><br>Case IPR2019- XXXX, US Patent No. 6,397,186<br>United States Patent and Trademark Office                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Declarations in support of invalidity in the context of an IPR.                                   | Retained by Arnold & Porter (contact: Jeffrey Miller) representing Samsung. This is an IPR related to patents for speech interfaces. This case is closed.                                                                                   |
| 12/2020 - 12/2022 | <b>Open Text Corp. v. Hyland Software, Inc.</b><br>Case No. 8:20-cv-02116-DOC-ADS<br>In the United States District Court for the Central District of California Southern Division                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Declarations supporting claim construction; expert reports; depositions.                          | Retained by King & Spalding LLP (contact: Brit Davis) representing Open Text. This is a patent dispute involving technology related to digital content management. This case is settled.                                                    |
| 05/2020 - 12/2021 | <b>Nice LTD and Mattersight Corp. v. Callminer, Inc.</b><br>Case No. 18-2024-RGA-SRF<br>In the United States District Court for the District of Delaware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Declarations.                                                                                     | Retained by DLA Piper LLP (contact: Tiffany Miller) representing Callminer, Inc. This is a patent dispute involving technology related to telephony integration. This case was settled.                                                     |
| 10/2019 - 06/2021 | <b>Freshub, Inc., Freshhub, LTD. v. Amazon.com inc., Amazon Digital Services, LLC, Prime Now, LLC, Whole Foods Market Inc., Whole Foods Market Services, Inc.</b><br>Case A-19-CV-00885-ADA<br>In the United States District Court for the Western District of Texas                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Expert report on infringement; expert report on validity; depositions; <b>testimony at trial.</b> | Retained by Kramer Levin (contact: Paul Andre) representing Freshub. This is a patent dispute concerning smart kitchen voice technologies. Testified at trial. The patents were found to be valid and not infringed.                        |
| 03/2020 - 05/2022 | <b>Broadcom Corporation, et al. v. Netflix, Inc.</b><br>Case No. 3:20-cv-04677-JD<br>In the United States District Court for the Northern District of California San Francisco Division                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Expert reports.                                                                                   | Retained by Thompson Knight (contact: Nadia Haghighatian). This is a patent case involving streaming content. This case is ongoing, but I am no longer involved.                                                                            |
| 06/2019 - 03/2022 | <b>Roku, Inc.</b> petition for <i>inter partes</i> review of US 7,821,505; 7,787,309; 7,821,504; Attorney Docket No. 48331.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Declarations, reply declarations, and a deposition.                                               | Retained by Haynes and Boone (contacts: Raghav Bajaj and Philip Woo) representing Roku, Inc. This is a patent case involving user interfaces on handheld remote controls.                                                                   |
| 04/2019 - present | <b>Vimeo, Inc and IAC/InterActiveCorp, v. British Telecommunications plc, IPR2019-00833</b><br>Case 1:18-vc-003366-VAC-CJB (D. Del.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Filed several declarations.                                                                       | Retained by McDonnell Boehnen Hulbert & Berghoff (contact: Jeffrey P. Armstrong) representing British Telecom. This is a patent case in district court as well as an IPR. This case is ongoing.                                             |
| 05/2018 - 12/2020 | <b>Retailmenot, Inc. v. Honey Science Corp.</b><br>Case no. 18-937(CFC)(MPT)<br>In the United States District Court for the District of Delaware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Expert declarations; help with infringement contentions; expert report; deposition.               | Retained by Kirkland & Ellis (contact: Christopher DeCoro) representing Retailmenot. This is a patent case involving ecommerce websites for shopping. The case was settled.                                                                 |
| 01/2017 - 01/2020 | <b>Koninklijke Philips N.V. et al. v. Acer Inc. et al.,</b><br>Case No. 15-1170-GMS<br><b>Koninklijke Philips N.V. et al. v. ASUSTeK Computer Inc. et al.,</b><br>Case No. 15-1125-GMS<br><b>Koninklijke Philips N.V. et al. v. Double Power Tech. et al.,</b><br>Case No. 15-1130-GMS<br><b>Koninklijke Philips N.V. et al. v. HTC Corp. et al.,</b><br>Case No. 15-1126-GMS<br><b>Koninklijke Philips N.V. et al. v. Southern Telecom Inc.,</b><br>Case No. 15-1128-GMS<br><b>Koninklijke Philips N.V. et al. v. Visual Land Inc.,</b><br>Case No. 15-1127-GMS<br><b>Koninklijke Philips N.V. et al. v. YiFang USA, Inc.,</b><br>Case No. 15-1131-GMS<br>In the United States District Court for the District of Delaware | Expert reports and depositions.                                                                   | Retained by Fitzpatrick, Cella, Harper & Scinto and Venable (contacts: Christopher Gerson or Jonathan Sharret) representing Koninklijke Philips N.V. and U.S. Philips Corporation. This was a patent dispute. The case ended in settlement. |

|                   |                                                                                                                                                                                                                                                                    |                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 03/2018 - 02/2019 | <i>Alarm.com et al v. SecureNet Technologies LLC</i> ,<br>Case No. 1:15-cv-00807-GMS<br>In the United States District Court for the District of Delaware                                                                                                           | Four expert reports on invalidity and non-infringement; analysis of source code; two depositions; <b>testimony at trial.</b>                   | Retained by Cooley LLP (contact: Erik B. Milch) representing SecureNet Technologies. This case was a patent case involving home security products and internet technologies. I was handling both non-infringement and invalidity. We prevailed at trial.                                                                                             |
| 01/2018 - 09/2018 | <i>Ameranth, Inc. v. Pizza Hut, Inc., et al.</i><br>Case No. 11-cv-1810 JLS<br>In the United States District Court Southern District of California                                                                                                                 | Expert report and deposition.                                                                                                                  | Retained by Baker Botts LLP (contact: Michael E. Knierim) representing Grubhub, Inc. and Seamless North America, LLC. This was a patent case involving data processing in the hospitality industry. I was asked to provide opinions concerning invalidity on a variety of grounds. We prevailed on a motion for summary judgment of unpatentability. |
| 04/2018 - 09/2021 | <i>MModal Services Ltd. v. Nuance Communications, Inc.</i><br>Case No. 1:18-cv-00901-WMR<br>In the United States District Court for the Northern District of Georgia Atlanta Division                                                                              | Declaration regarding claim terms; deposition. Expert report concerning non-infringement; expert report concerning invalidity; deposition.     | Retained by Weil, Gotshal & Manges LLP (contact: Sudip Kundu) representing Nuance Communications, Inc. This is a patent case involving speech recognition technology. I have prepared a report regarding certain claim terms. This case settled shortly before trial.                                                                                |
| 04/2018 - 04/2022 | <i>BookIT Oy Ajanvarauspalvelu v. Bank of America Corporation and Bank of America, N.A.</i><br>Case No. 3:17-cv-02557-K<br>In The United States District Court for the Northern District of Texas Dallas Division                                                  | Declarations regarding claim terms.                                                                                                            | Retained by Winston & Strawn, LLP representing Bank of America. This is a patent case. I am involved with a number of invalidity issues. This case settled favorably to the client.                                                                                                                                                                  |
| 08/2017- 06/2018  | <i>Darren Pederson v. Apple Inc.</i><br>Case No. 1:12-cv-235530<br>In the Santa Clara County Superior Court                                                                                                                                                        | Declaration in support of opposition to class certification; deposition.                                                                       | Retained by Morrison & Foerster LLP (contact: David M. Walsh) representing Apple, Inc. This is a class action case regarding the operation of Apple TV products. I was involved with a number of issues around class certification.                                                                                                                  |
| 01/2017 - 04/2019 | <i>Koninklijke Philips N.V. et al. v. Acer Inc. et al.</i><br>Case No. 15-1170-GMS<br>In the United States District Court for the District of Delaware                                                                                                             |                                                                                                                                                | Retained by Venable LLP representing Koninklijke Philips N.V. et al.                                                                                                                                                                                                                                                                                 |
| 03/2016 - 01/2018 | <i>Doug Baird, Goug Hesse and Bob Schmitt on Behalf of Blinkmind, Inc. v. Joe Baird, Nathan Stratton, Michael Tessler, Exario Networks Inc, and Broadsoft, Inc.</i><br>Case No. 2015-16576<br>In The District Court of Harris County, TX, 270th Judicial District. | Analysis of source code and documents related to allegations of copying. Expert report; deposition.                                            | Retained by Cooley LLP (contact: Jon Graves) representing Broadsoft. This case involves allegations of theft of trade secrets and copying. The case settled.                                                                                                                                                                                         |
| 11/2015 - 06/2017 | <i>Phoenix Technologies LTD. v. VMware, Inc.</i><br>Case No. 15- cv-014140-HSG<br>In The United States District Court North District of California                                                                                                                 | Expert report regarding a number of issues having to do with issues related to the definition of terms; deposition; <b>testimony at trial.</b> | Retained by Cooley LLP (contact: Whitty Somvichian) representing Phoenix Technologies. This is a contracts matter involving copyright. I offered opinions related to the meaning of certain terms used in a contract.                                                                                                                                |
| 05/2015 - 05/2015 | <i>Chestnut Hill Sound, Inc. v. Apple Inc.</i><br>Case No.15-cv-261 (D. Del.)<br>In The United States District Court for the District of Delaware                                                                                                                  | Declaration in support of Apple's opposition to preliminary injunction.                                                                        | Retained by Desmarais LLP (contact: Alan Kellman) representing Apple Inc. This is a patent matter involving control of multimedia streams in home entertainment networks.                                                                                                                                                                            |

|                      |                                                                                                                                                                                                                |                                                                                                                                           |                                                                                                                                                                                                                                                                                               |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 04/2015 -<br>07/2016 | <i>Mobile Telecommunications Technologies, LLC v. BlackBerry Corporation</i><br>Case No. 3:12-cv-01652-M (N.D. Tex.)<br>In the United States District Court for the Northern District of Texas Dallas Division | Expert report on non-infringement and invalidity; deposition; <b>testimony at trial.</b>                                                  | Retained by McDermott Will & Emery (contact: Leigh Martinson) representing Blackberry. I am handling invalidity as well as non-infringement. This is a patent case involving a number of issues related to smartphones and messaging. Testified at trial. We prevailed.                       |
| 03/2015 -<br>03/2017 | <i>WAG Acquisition LLC v. Gattyan S.a.r.l. et al.</i><br>Case No. 2:14-cv-2832-ES-JAD (D. N.J.)<br>In the United States District Court District of New Jersey                                                  | Declarations in four IPRs; deposition.                                                                                                    | Retained by Baker & McKenzie LLP (contacts: Kevin O'Brien and Matt Dushek) representing the defendants. This is a patent matter involving streaming media. I submitted declarations in four IPRs in this case.                                                                                |
| 02/2015 -<br>02/2017 | <i>Comcast Cable Communications LLC, et al. v. Sprint Communications Company L.P. et al.</i> ,<br>Case No. 2:12-cv-0859 (E.D. Pa)                                                                              | Expert report on invalidity; deposition; <b>testimony at trial.</b>                                                                       | Retained by McGuire Woods LLP (contact: George J. Barry III) representing Sprint Inc. This is a patent matter involving the architecture of messaging servers in a cell phone network.                                                                                                        |
| 12/2014 -<br>05/2015 | <i>Enterprise Systems Technologies S.a.r.l. v. Apple Inc.</i><br>C.A. No. 1:14-cv-00765-UNA<br>In the United States District Court for the District of Delaware                                                | Declaration submitted for IPR.                                                                                                            | Retained by Ropes & Gray LLP (contact: Stefan Geirhofer) representing Apple Inc. This was a patent matter involving a district court case, an ITC case, and an IPR. The technology mobile messaging. This case settled.                                                                       |
| 11/2014 -<br>04/2015 | <i>Solocron Media, LLC v. Verizon Communications Inc. , et al</i><br>Case No. 2:13-cv-1059 (E.D. Tex.)<br>In the United States District Court Eastern District of Texas Marshall Division                      | Expert report on invalidity.                                                                                                              | Retained by Wiley Rein LLP (contact: Scott Felder) representing Verizon. This was a patent matter. I prepared a report on invalidity and assisted with a report on non-infringement. This case terminated favorably for Verizon before I was deposed.                                         |
| 10/2014 -<br>02/2015 | <i>Recogni Corp, LLC v. Nintendo Co. Ltd. , et al.</i><br>Case No. 2:12-cv-01873-RAJ<br>In the U.S. District Court Western District of Washington                                                              |                                                                                                                                           | Retained by Orrick, Herrington & Sutcliffe LLP (Contact: Doc Daybell) representing Nintendo Co. Ltd.                                                                                                                                                                                          |
| 07/2014 -<br>01/2016 | <i>Aylus Networks, Inc. v. Apple Inc.</i><br>Case No: 3:13-cv-04700-EMC.<br>In the United States District Court Northern District of California San Francisco Division                                         | Declarations in support of claim construction as well as summary judgment; expert reports on non-infringement and invalidity; deposition. | Retained by DLA Piper (contact: Mark Fowler) representing Apple, Inc. I was handling non-infringement as well as invalidity. This was a patent matter involving control of multimedia streams in home entertainment networks. This case was dismissed on summary judgment favorable to Apple. |
| 5/2014 -<br>10/2014  | <i>Jobdiva, Inc. v. Monster Worldwide, Inc.</i><br>Case no: 13 Civ. 8229 (KBF)<br>In the United States District Court for the Southern District of New York                                                    | Declaration on infringement; deposition.                                                                                                  | Retained by Kirkland and Ellis (contact: James Marina) representing Jobdiva. This was a patent matter involving methods of search and display of resumes. I offered a declaration that was most of an expert report. This case settled.                                                       |
| 12/2013 -<br>06/2014 | <i>Straight Path IP Group, Inc., v. LG Electronics, Inc. et.al</i><br>C.A. No. 1:13-cv-00933<br>Investigation No. 337-TA-892                                                                                   | Expert report on non-infringement; deposition.                                                                                            | Retained by Finnegan (contact: Aidan Skoyles) representing LG Electronics, Inc. This was a patent matter regarding smart televisions. This case has been stayed.                                                                                                                              |
| 11/2013 -<br>12/2013 | <i>Glaxosmithkline, LLC v. Genentech, Inc.</i><br>Case No: 10-799-GMS.<br>In the United States District Court for the District of Delaware                                                                     | Expert report on an evidentiary matter; deposition.                                                                                       | Retained by Desmarais (contact: Xiao Li) representing GSK. I offered opinions regarding the quality of certain metadata information associated with several files at issue in the case.                                                                                                       |
| 9/2013 -<br>9/2014   | <i>Profectus Technology LLC v. Huawei Technologies Co. LTD, et al.</i><br>Case No. 6:11-cv-00474.<br>In the United States District Court for the Eastern District of Texas Tyler Division                      | Expert report on non-infringement.                                                                                                        | Retained by Baker Botts (contact: Tammy Pennington) representing Dell. This patent matter dealt with technologies used in electronic picture frames. This case settled.                                                                                                                       |

|                   |                                                                                                                                                                                                                                                                                                            |                                                                             |                                                                                                                                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9/2013 - 3/2014   | <i>Black Hills Media v. Samsung, LGE et al., Certain Digital Media Devices, including Televisions, Blu-Ray Disc Players, Home Theater Systems, Tablets and Mobile Phones, Components Thereof and Associated Software.</i><br>Investigation No. 337-TA-882.<br>United States International Trade Commission | Expert report on non-infringement; deposition; <b>testimony at hearing.</b> | Retained by Finnegan (contact: Houtan Esfahani) representing LGE. This was a patent case involving cell phone power systems.                                                                                                                             |
| 6/2013 - 2/2015   | <i>OpenText S.A. v. Alfresco Software LTD; Alfresco Software, Inc.; and Carahsoft Technology Corporation.</i><br>Case No. 2:13CV320AWA/LRL.<br>In the United States District Court for the Eastern District of Virginia                                                                                    | Expert reports on infringement and validity; depositions; tech tutorial.    | Retained by Cooley LLP (contact: Frank Pietrantonio) representing OpenText. My patents were dropped from trial.                                                                                                                                          |
| 05/2013 - present | <i>Hartford Fire Insurance Company v. Progressive Corporation and Progressive Casualty Insurance Company.</i><br>Case No. 1:12- cv-02444.<br>In the United States District Court for the Northern District of Ohio Eastern Division                                                                        | Expert report on claim construction; deposition.                            | Retained by Baker Botts (contact: Robert Scheinfeld) representing Hartford. I am handling both infringement as well as validity.                                                                                                                         |
| 10/2012 - 04/2013 | <i>MobileMedia Ideas, LLC v. HTC Corporation and HTC America, Inc.</i><br>In the United States District Court for the Eastern District of Texas, Marshall Division                                                                                                                                         | Expert reports; deposition.                                                 | Retained by Desmarais LLP (contact: Alan Kellman) representing MMI. This is a patent dispute involving user interfaces to cell phones. I am handling both infringement and validity.                                                                     |
| 10/2012 - 04/2014 | <i>Nokia Corporation, Nokia Inc., and Intellisync Corp v. HTC. Certain Electronic Devices, Including Mobile Phones and Tablet Computers, and Components Thereof.</i><br>Investigation No. 337-TA-847.<br>United States International Trade Commission                                                      | Expert reports; depositions; <b>testimony at hearing.</b>                   | Retained by Desmarais LLP (contact: Alan Kellman) representing Nokia. This was a patent dispute involving user interfaces to cell phones. I handled both infringement and validity. My patent was dropped from the case during the hearing.              |
| 09/2012 - 04/2017 | <i>Intellectual Ventures I, LLC et al. v. AT&amp;T Mobility LLC et al.</i><br>Civil Action No. 12-CV-193-LPS (D.Del.)                                                                                                                                                                                      |                                                                             | Retained by Baker Botts (contact: Robert Maier) representing AT&T Mobility, LLC.                                                                                                                                                                         |
| 8/2012 - 10/2015  | <i>Potter Voice Technologies, LLC v. Apple Inc. et al.</i><br>CV 1:12-cv-01096-REB-CBS<br>In The United States District Court for the District of Colorado                                                                                                                                                 | Declaration in support of summary judgment; expert reports.                 | Retained by Cooley LLP (contact: Timothy Teter) representing Apple Inc. This was a patent dispute involving Natural Language Processing on smartphones. I handled both infringement and validity. This case was favorably dismissed on summary judgment. |
| 08/2012 - 10/2014 | <i>OpenTV, Inc. v. Netflix Inc.</i><br>Case No. 3:14-cv-01525<br>In the United States District Court for the District of Delaware                                                                                                                                                                          | Declaration regarding a motion for summary judgment.                        | Retained by Kirkland & Ellis LLP (contact: Matthew Topic) representing OpenTV. I submitted a declaration in opposition to a motion for summary judgment regarding section 101 issues.                                                                    |
| 08/2012 - 12/2012 | <i>J2 Global Communications, Inc. v. EasyLink Services International Corp.</i><br>Case No. 09-4189-DDP (AJWx)<br>In The United States District Court Central District of California Western Division                                                                                                       |                                                                             | Retained by Perkins Coie LLP (contact: Timothy Carroll) representing EasyLink Corp. I handled both infringement and validity. This was a patent dispute regarding enterprise fax and messaging systems.                                                  |
| 06/2012 - 8/2017  | <i>EasyWeb Innovations, LLC v. Twitter, Inc.</i><br>Civil Action No CV 11-4550-JFB-WDW.<br>In The United States District Court for the Eastern District of New York                                                                                                                                        | Expert reports; deposition.                                                 | Retained by Desmarais LLP (contact: Alan Kellman) representing EasyWeb. This is a patent dispute involving messaging technologies. I am handling both infringement and validity.                                                                         |

|                   |                                                                                                                                                                                                                                               |                                                                                                |                                                                                                                                                                                                                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 06/2012           | <b>Cisco</b>                                                                                                                                                                                                                                  | Declaration.                                                                                   | Retained by Haynes and Boone LLP (contact: Andrew Ehmke) representing Cisco. This was an IPR case and I submitted a declaration in the matter.                                                                                                                                                                              |
| 02/2012 - 06/2014 | <i>Emblaze LTD v. Apple Inc.</i><br>Case No 4:11-CV-01079 SBA.<br>In The United States District Court for the Northern District of California                                                                                                 | Markman tutorial; Expert report on non-infringement; tech tutorial; <b>testimony at trial.</b> | Retained by Greenberg Traurig LLP (contact: James DeCarlo) representing Apple, Inc. The case was ultimately tried by DLA Piper (contact: Mark Fowler). This was a patent dispute. The case involved technology for distribution of multimedia over the Internet. The trial concluded with the jury finding no infringement. |
| 12/2011 - 04/2013 | <i>Apple Inc. v. Samsung Electronics Co, LTD.</i><br>Case No. CV12-00630<br>In The United States District Court for the Northern District of California San Jose Division                                                                     | Expert declaration; deposition.                                                                | Retained by Gibson Dunn LLP (contact: Joshua Furman) representing Apple Inc. This is a patent dispute involving multi-database search on a mobile device. I am handling both infringement and validity. We received a pre-trial injunction on the products in question.                                                     |
| 12/2011 - 08/2012 | <i>NorthMobile Tech, LLC v. Simon Property Group, Inc.</i><br>Case No. 3:11-cv-287<br>In The United States District Court Western District of Wisconsin                                                                                       | Expert report; declarations.                                                                   | Retained by Perkins Coie LLP (contact: Timothy Carroll) representing Simon Property Group. This was a patent dispute involving a location based marketing application on smartphones. I am handling both infringement and validity. We prevailed pretrial.                                                                  |
| 11/2011 - 09/2015 | <i>Oasis Research, LLC v. ADrive LLC, et al.</i><br>Case No. 4:10-CV-435-MHS-ALM<br>In The United States District Court for the Eastern District of Texas Sherman Division                                                                    | Expert reports; deposition.                                                                    | Retained by Desmarais LLP (contact: Alan Kellman) representing Oasis Research LLC. I am handling both infringement and validity. This is a patent dispute regarding on line backup and storage. This case settled.                                                                                                          |
| 08/2011 - 06/2014 | <i>Apple Inc. and Next Software, Inc. v. Motorola, Inc. and Motorola Mobility, Inc.</i><br>Case No. 10-CV-662 (BBC)<br>In The United States District Court for The Western District of Wisconsin                                              | Expert reports.                                                                                | Retained by Weil, Gotshal & Manges LLP (contacts: Kevin Kudlac and Elizabeth Weiswasser) representing Apple, Inc. This was a patent dispute. The case involved technology for the interface of DSPs in cell phones. I handled both infringement as well as validity. This case was dismissed pretrial by Judge Posner.      |
| 06/2011 - 02/2012 | <i>Creative Kingdoms, LLC and Medici Portfolio LLC v. Nintendo Co. Ltd. Certain video game systems and Wireless controllers and Components thereof.</i><br>Investigation No.337-TA-770<br>In The United States International Trade Commission | Expert report; deposition; <b>testimony at hearing.</b>                                        | Retained by Cooley LLP (contacts: Tim Teter and Matthew Brigham) representing Nintendo Co. Ltd. This was a patent dispute. The case involved technology used in wireless and motion sensing controllers. I handled invalidity. We prevailed at the hearing.                                                                 |
| 02/2011 - 11/2011 | <i>WiAv Solutions LLC v. Motorola Mobility, Inc, Nokia Corp., Nokia, Inc, Sony Ericsson Mobile</i><br>Civil Action No: 3:09-cv-447-LO<br>In The United States District Court for The Eastern District of Virginia                             | Expert report; deposition.                                                                     | Retained by Finnegan, Henderson, Farabow, Garrett & Dunner LLP (contacts: Kenie Ho and Christopher Schultz) representing WiAv Solutions LLC. This was a patent dispute. The case involved technology for speech codecs used in GSM cell phones. I handled the infringement side of the case. This case settled.             |
| 08/2010 - 04/2011 | <i>Apple Inc. v. Nokia Corporation and High Tech Computer Corp. (HTC). Certain Personal Data and Mobile Communications Devices and Related Software.</i><br>Investigation No. 337-TA-710<br>United States International Trade Commission      | Expert reports; depositions; <b>testimony at hearing.</b>                                      | Retained by Kirkland & Ellis LLP (contacts: Marc Sernel and Eric Hayes) representing Apple Inc. This was a patent dispute. The case involved technology for the interface of DSPs in cell phones. I handled both infringement as well as validity.                                                                          |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 07/2010 -<br>11/2010 | <i>ACQIS LLC v. Appro International, Inc., Clear Cube Technology, Inc., Dell Inc., Fujitsu Computer Systems Corp., Hitachi America, Ltd., Hewlett-Packard Co., International Business Machines Corp., NEC Corp. of America, NEX Computers, Inc., Sun Microsystems, Inc. and Super Micro Computer, Inc.</i><br>Case No. 6:06-cv-00148<br>In the United States District Court for the Eastern District of Texas | Expert report on invalidity and non-infringement.                       | Retained by Covington & Burling LLP (contact: Chris Martiniak) representing Hewlett Packard. This was a patent matter involving computer blade servers. The case settled.                                                                                                                                                                                                                              |
| 04/2010 -<br>06/2010 | <i>Illinois Computer Research LLC v. Harpo Productions, Inc. et al</i><br>Case Number: 1:2008cv07322<br>In The United States District Court for The Northern District of Illinois Eastern Division                                                                                                                                                                                                            | Expert report; deposition.                                              | Retained by Jackson Walker LLP (contacts: Michael Locklarand Charles Babcock) representing Harpo Productions, Inc. This was a patent dispute. The case involved technology for display of books on a website. This case settled.                                                                                                                                                                       |
| 02/2010 -<br>06/2010 | <i>Motorola Inc. v. Research Motion Limited et al</i><br><i>Certain wireless communication server system software, wireless handheld devices and battery packs.</i><br>Investigation No. 337-TA-706<br>United States International Trade Commission                                                                                                                                                           | Expert report.                                                          | Retained by Ropes & Gray (contacts: Paul M. Schoenhard and Steven Pepe) representing Motorola, Inc. This was a patent dispute. The case involved technology used in pagers and cell phones as well as their servers. This case settled.                                                                                                                                                                |
| 08/2009 -<br>10/2010 | <i>Balthaser Online, Inc. v. Network Solutions, LLC.</i><br>Civil Action No. 2:08-cv-430<br>In The United States District Court Eastern District of Texas Marshall Division                                                                                                                                                                                                                                   | Expert report.                                                          | Retained by Dickstein Shaprio LLP (contacts: Alfred R. Fabricant and Lawrence C. Drucker) representing Balthaser Online, Inc. This was a patent dispute. The case involved technology for the display of rich media applications on a web site. This case settled.                                                                                                                                     |
| 05/2009 -<br>05/2010 | <i>Nuance Communications Inc. et al v. Tell me Networks Inc.</i><br>Case Number: 1:2006cv00105<br>In The United States District Court for The District of Delaware                                                                                                                                                                                                                                            | Expert report.                                                          | Retained by McKool Smith (contact: Luke F. McLeroy) representing Nuance Communications. This was a patent dispute. The technology involved techniques for using speech recognition in telephone information systems. This case ended in summary judgment for the defendant.                                                                                                                            |
| 12/2008 -<br>12/2009 | <i>TruePosition Inc. v. Andrew Corp, C.A.</i><br>Case No. 05-0747-SLR (D. Del)<br>U.S. District Court for the District of Delaware                                                                                                                                                                                                                                                                            | Declaration; expert report.                                             | Retained by Kirkland & Ellis LLP (contact: Avinash Lele) representing Andrew Corp, C.A. Patent infringement case concerning technology for determining location of a cell phone using information from several cell phone towers. I provided an analysis of a workaround approach.                                                                                                                     |
| 10/2008 -<br>01/2010 | <i>RealTime Data LLC. v. Packeteer, Inc.</i><br>Case No. 6:2008cv00144<br>U.S. District Court for the Eastern District of Texas                                                                                                                                                                                                                                                                               | Expert report; depositions; trial prep.                                 | Retained by Ropes & Gray LLP (contact: Anthony Pastor) representing RealTime Data, LLC. Patent infringement case concerning data compression, storage, and transmission. This case settled on first day of trial.                                                                                                                                                                                      |
| 10/2008 -<br>09/2009 | <i>Thomson Reuters (Scientific) Inc. v. David A.Von Moll, Comptroller of the Commonwealth of Virginia and George Mason University</i><br>Civil Action No. CL2008-17114<br>Circuit Court of Fairfax County Virginia                                                                                                                                                                                            | Expert report.                                                          | Retained by Edwards Angell Palmer & Dodge LLP (contacts: Glenn Pudelka and Barry Kramer) representing Thomas Reuters (Scientific) Inc. Contracts dispute centered around allegations of reverse engineering of software. This case ended in summary judgment.                                                                                                                                          |
| 04/2008 -<br>12/2008 | <i>International Business Machines Corporation v. Asustek Computer, Inc. Certain Computer Products, Computer Components and Products contain Same.</i><br>Investigation No. 337-TA-628<br>United States International Trade Commission                                                                                                                                                                        | Expert reports; declarations; depositions; <b>testimony at hearing.</b> | Retained by Cadwalader Wickersham & Taft LLP (contacts: John Moehringer and Christopher Hughes) representing IBM in this matter. This was an US ITC investigation regarding infringement of a number of IBM patents by computers produced and sold by Asustek. The technology involved computer control of cooling systems for computers. I was involved with infringement as well as validity issues. |

|                   |                                                                                                                                                                                                              |                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10/2007 - 05/2008 | <b><i>Lucent, Alcatel-Lucent, and Multimedia Patent Trust v. Microsoft</i></b><br>Case no. 06-CV- 0684-H (LAB)<br>U.S. District Court for the Southern District of California                                | Expert reports; depositions;<br><b>testimony at trial.</b>                   | Retained by Kirkland & Ellis LLP (representing Lucent Technologies) (contacts: Robert Appleby and John Desmarais) and Baker Botts LLP (representing Alcatel-Lucent). I advised on infringement as well as validity of U.S. Patents 5,838,319 and 5,977,971. Gave trial testimony regarding invalidity of the '971 patent: jury found the patent was invalid.                                                                                                                                |
| 03/2000 - 01/2009 | <b><i>National Music Publishers' Association et al. v. XM Satellite Radio Inc.</i></b><br>Civil Action 06-CV-3733(LAK)<br>In The U.S. District Court for the Southern District of New York                   |                                                                              | Retained by Gibson Dunn & Crutcher LLP representing National Music Publishers' Association. Copyright dispute concerning the impact of various XM Satellite Radio products. I provided an analysis of source code and functionality of several XM devices.                                                                                                                                                                                                                                  |
| 06/2006 - 02/2007 | <b><i>Lucent v. Gateway, Microsoft, Dell</i></b><br>Case no. 02-CV-2060-B (LAB)<br>Case no. 03-CV-0699-B (LAB)<br>Case no. 03-CV-1108-B (LAB)<br>U.S. District Court for the Southern District of California | Expert reports; depositions;<br><b>testimony at trial.</b>                   | Retained by Kirkland & Ellis LLP representing Lucent Technologies (contacts: Robert Appleby and John Desmarais). I worked on the infringement of Patents 5,341,457 and 5,627,938 as well as validity of these patents. At trial, I testified to regarding infringement of the '457, '938 and '080 patents. This matter concluded with a successful verdict and an award to Lucent of \$1.5 billion.                                                                                         |
| 02/2006           | <b><i>Board of Regents of the University of Texas v. Benq America Corp et al.</i></b><br>Civil Action No. A:05CA181<br>U.S. District Court for the Western District of Texas                                 | <b>Markman Hearing Testimony;</b> Expert reports; deposition; tech tutorial. | Retained by Quinn Emanuel Urquhart Oliver & Hedges LLP (contacts: Evette Pennypacker and Kevin Johnson) representing Benq America et al. Patent infringement. For a Markman (claim construction) hearing, prepared and presented a technology tutorial and testified before a special master. Prepared reports and gave deposition regarding invalidity and inoperability technology in the patent at issue.<br>Claim construction hearing led to summary judgment in Benq America's favor. |
| 2006              | <b><i>Telefonaktiebolaget LM Ericsson et al. v. Samsung Electronics Company Ltd.</i></b><br>Investigation No. 337-TA-577<br>U.S. International Trade Commission                                              | Expert reports and depositions.                                              | Retained by Kirkland & Ellis LLP (contacts: Bao Nguyen, Adam Gill and Michael Pieja) representing Samsung in several patent infringement claims brought by Ericsson. Claims involved technologies for messaging, speech encoding, and speech recording within various GSM cell phones. This case settled just prior to hearing.                                                                                                                                                             |
| 07/2005 - 02/2006 | <b><i>Encyclopedia Britannica Inc. v. Alpine Electronics of America Inc. et al.</i></b><br>Civil Action No. 05-359<br>U.S. District Court for the Western District of Texas                                  | Expert report; deposition.                                                   | Retained by Baker Botts LLP (contact: David Wille) representing Encyclopedia Britannica, Inc. Patent infringement. Prepared report on the definiteness of certain claim terms, and was deposed on this matter. This case is ongoing but inactive.                                                                                                                                                                                                                                           |
| 2005 - present    | <b><i>Advanced Analytics Inc. v. Citigroup Global Markets Inc.</i></b><br>Case No. 04 Civil 3531 (LTS)<br>U.S. District Court for the Southern District of New York                                          | Declarations and expert reports; deposition.                                 | Retained by Cleary Gottlieb Steen & Hamilton LLP (contacts: David Williams and Chris Moore) representing Citigroup Global Markets, Inc. Theft of trade secrets. I have been involved in software analysis in this case. The case involved software used to price complex financial instruments. Refuting the claims required software analysis as well as statistical analysis of certain elements of the systems involved. This case pending.                                              |
| 05/2005 - 09/2005 | <b><i>Atronic International GMBH v. SAI Semi-specialists of America Inc.</i></b><br>Case No. 03-CV-4892 (TCP) (MLO)<br>U.S. District Court for the Eastern District of New York                              | Expert report; deposition.                                                   | Retained by Ford Marrin Esposito Witmeyer & Gleser LLP (contact: Edward M. Pinter) representing Atronic International. Contracts dispute. I have acted primarily to rebut another witness regarding what would have been reasonable behavior for a customer of an electronic parts supplier. This case settled.                                                                                                                                                                             |

|                      |                                                                                                                                                                                                                       |                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 02/2005 -<br>03/2006 | <i>Tivo Inc. v. <b>Echostar Communications Corporation</b></i><br>Case No. 2-04cv01 DF<br>U.S. District Court for the Eastern District of Texas                                                                       | Expert report; deposition;<br><b>testimony at trial.</b>  | Retained by Morrison & Foerster (contact: Karl Kramer) representing Echostar. This case involved digital video recorder (DVR) technology. My work focused on the invalidity of the Tivo patent. I found many pieces of prior art including complete systems that were presented at trial. Tivo prevailed at trial. Most of the claims were subsequently found invalid on re-exam. This case has been the subject of many appeals.                                                                                                                                                                                                            |
| 12/2004 -<br>05/2006 | <i>Foundry Networks Inc. v. <b>Lucent Technologies Inc.</b></i><br>Case No. 2:04-CV-40 (TJW) (E.D. Tex.)<br>U.S. District Court for the Eastern District of Texas                                                     | Expert reports.                                           | Retained by Kirkland & Ellis LLP (contacts: Jenny Lee and Jeanne Heffernan) representing Lucent Technologies. I advised on infringement as well as validity of U.S. Patent 5,649,131. In addition to generating several reports, I supported the drafting of motions and declarations. This case settled shortly before trial.                                                                                                                                                                                                                                                                                                               |
| 07/2004 -<br>01/2005 | <i>Voice Capture Inc. v. <b>Intel Corporation</b>, Dialogic Corporation, and Nuance Communications, Inc.</i><br>No. 4:04-cv-40340<br>U.S. District Court for the Southern District of Iowa                            | Expert report.                                            | Retained by Gary Cary (contact: Edward Sikorsky) representing Intel Corporation. The case involved Voice Capture's allegation of patent infringement by Intel in the area of interactive voice response systems. In producing an invalidity report on the patent, I analyzed the patent and prior art in great detail. I also provided an expert report on invalidity and an analysis of a rebuttal report. The case settled.                                                                                                                                                                                                                |
| 05/2004 -<br>03/2005 | <i>Dolby Laboratories Inc. v. <b>Lucent Technologies Inc.</b></i><br>Case No. C 01-20709 JF (RS)<br>U.S. District Court for the Northern District of California                                                       | Expert report.                                            | Retained by Kirkland & Ellis LLP (contact: Alan Kellman) representing Lucent Technologies. This case involved infringement of a number of Lucent's patents by Dolby's AC3 codec. The case settled.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 03/2003              | <i><b>Agere Systems Inc.</b> v. <i>Broadcom Corporation</i></i><br>Civil Action No. 03-3138<br>U.S. District Court for the Eastern District of Pennsylvania                                                           | Expert report.                                            | Retained by Kirkland & Ellis LLP (contacts: Bryan Hales and Edward Runyan). The case involved Agere's allegation of patent infringement by Broadcom in the area of speech compression used in various Broadcom telephone products. I analyzed the operation of a speech codec used in digital telephones; worked with counsel and other experts to prepare reports. This case settled.                                                                                                                                                                                                                                                       |
| 10/2001              | <i><b>AT&amp;T Corp.</b> v. <i>Microsoft Corporation</i></i><br>Civil Action No. 01 CV 4872 (WHP)<br>U.S. District Court for the Southern District of New York                                                        | Expert reports; deposition;<br><b>testimony at trial.</b> | Retained by Cooley Godward Kronish LLP (contacts: Frank Pietrantonio and Stephen Neal) representing AT&T. The case involved AT&T's allegation of patent infringement by Microsoft in the area of speech compression. I analyzed the operation of three speech codecs and worked with counsel and other experts to prepare reports. I was deposed and gave testimony at trial. After the presentation of our case, the matter settled; details of the settlement are confidential. Elements of this case reached the U.S. Supreme Court.                                                                                                      |
| 2000                 | <i>Data System Analysis Inc. v. <b>The Netplex Group Inc.</b>, Technology Development Systems Inc. and Xcellenet Inc.</i><br>Civil Action No. 97-4652 (JBS-RBK)<br>U.S. District Court for the District of New Jersey | Expert reports; deposition.                               | Retained by Saul Ewing LLP (contact: Michael Lampert) representing Netplex. Data Systems Analysis (DSA) brought suit against Netplex in a contract matter regarding software claimed by both companies. I was retained to analyze the disputed software and determine a method for computing damages. My expert report found that "functionality" and "effort required to create" were both better metrics than "number of lines of software", the measurement proposed by DSA. I was deposed for several days in this case, provided analysis of other expert reports and assisted in preparing counsel for depositions. This case settled. |

|                      |                                                                                                                                                                                    |                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 01/1998 -<br>01/2001 | <b><i>System Management Arts Inc. (SMARTS) v. Avesta Technologies Inc. and David Zager</i></b><br>97 Civil 8101 (RWS)<br>U.S. District Court for the Southern District of New York | Expert reports; deposition. | Initially retained by Kramer Levin Naftalis & Frankel LLP (contact: Thomas H. Moreland) representing SMARTS. In early 2000 SMARTS retained Proskauer Rose LLP (contact: Kenneth Rubenstein). The case involved a SMARTS patent in the area of automatic diagnostics of faults in communications networks. I analyzed an Avesta system with similar claimed capabilities and produced an expert report. I also gave deposition and participated extensively in technological analysis and strategic discussions of all aspects of the case. This case settled. |
| 1997                 | <b><i>Knowledge Based Technologies Inc. v. International Business Machines Corp.</i></b><br>Case No. 96-9461 (JSR)<br>U.S. District Court for the Southern District of New York    | Expert reports; deposition. | Retained by Morris, Nichols, Arsht & Tunnell LLP (contact: Karen Jacobs Loudon) representing Knowledge Based Technologies. Contract dispute regarding the application of fuzzy logic techniques. I generated an expert report that analyzed several forms of fuzzy logic software to determine whether the software was independently developed. I also was deposed in this case. This case settled.                                                                                                                                                          |