

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

ABSOLUTE SOFTWARE CORP. and ABSOLUTE SOFTWARE, INC.,  
Petitioners

v.

SOFTEX LLC,  
Patent Owner

---

Case IPR2024-00288  
U.S. Patent No. 8,506,649 B2  
Issue Date: August 13, 2013

Title: ELECTRONIC DEVICE SECURITY AND TRACKING SYSTEM AND  
METHOD

**PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 8,506,649 B2**

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

|      |                                                                                                                |    |
|------|----------------------------------------------------------------------------------------------------------------|----|
| I.   | MANDATORY NOTICES UNDER § 42.8(A)(1) .....                                                                     | 1  |
| A.   | Related Matters under § 42.8(b)(2) .....                                                                       | 1  |
| B.   | Real Party-In-Interest under § 42.8(b)(1).....                                                                 | 1  |
| C.   | Lead and Back-Up Counsel under § 42.8(b)(3) .....                                                              | 3  |
| D.   | Service Information .....                                                                                      | 4  |
| E.   | Power of Attorney .....                                                                                        | 4  |
| II.  | FEE PAYMENT .....                                                                                              | 4  |
| III. | REQUIREMENTS UNDER §§ 42.104 AND 42.108 AND<br>CONSIDERATIONS UNDER §§ 314(A) AND 325(D).....                  | 5  |
| A.   | Standing.....                                                                                                  | 5  |
| B.   | Identification of Challenge.....                                                                               | 5  |
| C.   | §§ 314(a) and 325(d) .....                                                                                     | 5  |
| IV.  | OVERVIEW OF THE '649 PATENT .....                                                                              | 10 |
| V.   | LEVEL OF ORDINARY SKILL IN THE ART .....                                                                       | 11 |
| VI.  | CLAIM CONSTRUCTION .....                                                                                       | 11 |
| VII. | THE CHALLENGED CLAIMS ARE UNPATENTABLE.....                                                                    | 12 |
| A.   | Prior Art.....                                                                                                 | 12 |
| 1.   | zTrace [EX1004-EX1028, EX1052-EX1053].....                                                                     | 12 |
| 2.   | Kesler [EX1029] .....                                                                                          | 17 |
| 3.   | Isikoff [EX1030] .....                                                                                         | 19 |
| 4.   | Bonnett [EX1031] .....                                                                                         | 20 |
| 5.   | Eckardt [EX1032] .....                                                                                         | 20 |
| B.   | Ground 1: Claims 1, 7, 9 and 15 are rendered obvious by<br>zTrace in view of Kesler, Isikoff and Bonnett ..... | 21 |
| 1.   | Independent claim 1 .....                                                                                      | 21 |
| (a)  | Limitation 1[a] .....                                                                                          | 21 |
| (b)  | Limitation 1[b].....                                                                                           | 21 |
| (c)  | Limitation 1[c] .....                                                                                          | 22 |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

|       |                                                                                                                |    |
|-------|----------------------------------------------------------------------------------------------------------------|----|
| (d)   | Limitation 1[c][i] .....                                                                                       | 27 |
| (e)   | Limitation 1[c][ii] .....                                                                                      | 30 |
| (f)   | Limitation 1[c][iii] .....                                                                                     | 33 |
| (g)   | Limitation 1[c][iv] .....                                                                                      | 35 |
| (h)   | Limitation 1[c][v] .....                                                                                       | 42 |
| (i)   | Limitation 1[c][vi] .....                                                                                      | 46 |
| (j)   | Limitation 1[d] .....                                                                                          | 47 |
| (k)   | Limitation 1[e] .....                                                                                          | 50 |
| (l)   | Limitation 1[f] .....                                                                                          | 56 |
| (m)   | Limitation 1[g] .....                                                                                          | 59 |
| 2.    | Independent claim 9 .....                                                                                      | 62 |
| (a)   | Preamble .....                                                                                                 | 63 |
| (b)   | Limitation 9[a] .....                                                                                          | 63 |
| (c)   | Limitation 9[b] .....                                                                                          | 64 |
| 3.    | Dependent claims 7 and 15 .....                                                                                | 65 |
| C.    | Ground 2: Claims 1, 7, 9 and 15 are rendered obvious by<br>zTrace in view of Kesler, Isikoff and Eckardt ..... | 66 |
| 1.    | Limitation 1[d] .....                                                                                          | 66 |
| 2.    | Limitation 1[e] .....                                                                                          | 67 |
| 3.    | Limitation 1[f] .....                                                                                          | 70 |
| 4.    | Limitation 1[g] .....                                                                                          | 70 |
| VIII. | NO SECONDARY CONSIDERATIONS OF NONOBVIOUSNESS .....                                                            | 72 |
| IX.   | CONCLUSION .....                                                                                               | 72 |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

| Exhibit<br>No. | Description of Document                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1001           | U.S. Patent No. 8,506,649 B2 issued to Apurva Mahendrakumar Bhansali et al. (filed July 11, 2006, issued Aug. 13, 2013) (“’649 patent”)                                                                                     |
| 1002           | File History of the ’649 patent                                                                                                                                                                                             |
| 1003           | Declaration of Dr. Nathaniel Polish                                                                                                                                                                                         |
| 1004           | zTrace Overview page:<br><a href="https://web.archive.org/web/20020802143350/http://www.ztrace.com:80/">https://web.archive.org/web/20020802143350/http://www.ztrace.com:80/</a>                                            |
| 1005           | zTrace zSecurity Suite page:<br><a href="https://web.archive.org/web/20020604051951/http://www.ztrace.com:80/zSecuritySuite.asp">https://web.archive.org/web/20020604051951/http://www.ztrace.com:80/zSecuritySuite.asp</a> |
| 1006           | zTrace Gold page:<br><a href="https://web.archive.org/web/20020810160306/http://www.ztrace.com:80/zTraceGold.asp">https://web.archive.org/web/20020810160306/http://www.ztrace.com:80/zTraceGold.asp</a>                    |
| 1007           | zTrace Gold Brochure:<br><a href="https://web.archive.org/web/20030319061040/http://ztrace.com/data_sheet/zTraceGold.pdf">https://web.archive.org/web/20030319061040/http://ztrace.com/data_sheet/zTraceGold.pdf</a>        |
| 1008           | zTrace zPass page:<br><a href="https://web.archive.org/web/20020604052039/http://www.ztrace.com:80/zPass.asp">https://web.archive.org/web/20020604052039/http://www.ztrace.com:80/zPass.asp</a>                             |
| 1009           | zTrace zPass Brochure:<br><a href="https://web.archive.org/web/20030510220600/http://www.ztrace.com/data_sheet/zPass.pdf">https://web.archive.org/web/20030510220600/http://www.ztrace.com/data_sheet/zPass.pdf</a>         |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

| Exhibit<br>No. | Description of Document                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                                                                                                               |
| <b>1010</b>    | zTrace zEncrypt:<br><a href="https://web.archive.org/web/20020604050748/http://www.ztrace.com:80/zEncrypt.asp">https://web.archive.org/web/20020604050748/http://www.ztrace.com:80/zEncrypt.asp</a>                           |
| <b>1011</b>    | zTrace zEncrypt Brochure:<br><a href="https://web.archive.org/web/20030510191741/http://www.ztrace.com/data_sheet/zEncrypt.pdf">https://web.archive.org/web/20030510191741/http://www.ztrace.com/data_sheet/zEncrypt.pdf</a>  |
| <b>1012</b>    | zTrace zControl page:<br><a href="https://web.archive.org/web/20020810155003/http://www.ztrace.com:80/zControl.asp">https://web.archive.org/web/20020810155003/http://www.ztrace.com:80/zControl.asp</a>                      |
| <b>1013</b>    | zTrace – How zControl Works page:<br><a href="https://web.archive.org/web/20020814064818/http://www.ztrace.com/zControlHow.asp">https://web.archive.org/web/20020814064818/http://www.ztrace.com/zControlHow.asp</a>          |
| <b>1014</b>    | zTrace – Why You Need zControl page:<br><a href="https://web.archive.org/web/20020613175359/http://www.ztrace.com/zControlWhy.asp">https://web.archive.org/web/20020613175359/http://www.ztrace.com/zControlWhy.asp</a>       |
| <b>1015</b>    | zTrace – zAssetTrack page:<br><a href="https://web.archive.org/web/20020604050138/http://www.ztrace.com:80/zAssetTrack.asp">https://web.archive.org/web/20020604050138/http://www.ztrace.com:80/zAssetTrack.asp</a>           |
| <b>1016</b>    | zTrace – How zAssetTrack Works page:<br><a href="https://web.archive.org/web/20020613174133/http://www.ztrace.com/zAssetTrackHow.asp">https://web.archive.org/web/20020613174133/http://www.ztrace.com/zAssetTrackHow.asp</a> |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

| Exhibit No. | Description of Document                                                                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1017        | zTrace – Why You Need zAssetTrack page:<br><a href="https://web.archive.org/web/20020613175056/http://www.ztrace.com/zAssetTrackWhy.asp">https://web.archive.org/web/20020613175056/http://www.ztrace.com/zAssetTrackWhy.asp</a>                                |
| 1018        | zTrace – Why You Need zTrace page:<br><a href="https://web.archive.org/web/20020613180259/http://www.ztrace.com:80/zTraceWhy.asp">https://web.archive.org/web/20020613180259/http://www.ztrace.com:80/zTraceWhy.asp</a>                                         |
| 1019        | zTrace – FAQ page:<br><a href="https://web.archive.org/web/20020405211735/http://www.ztrace.com:80/faq.asp">https://web.archive.org/web/20020405211735/http://www.ztrace.com:80/faq.asp</a>                                                                     |
| 1020        | zTrace – zGuarantee page:<br><a href="https://web.archive.org/web/20021002045822/http://www.ztrace.com:80/guarantee.asp">https://web.archive.org/web/20021002045822/http://www.ztrace.com:80/guarantee.asp</a>                                                  |
| 1021        | zTrace – Corporate page:<br><a href="https://web.archive.org/web/20020606100347/http://www.ztrace.com/Corporate.asp">https://web.archive.org/web/20020606100347/http://www.ztrace.com/Corporate.asp</a>                                                         |
| 1022        | zTrace – How zTrace Works page:<br><a href="https://web.archive.org/web/20020814065623/http://www.ztrace.com:80/zTraceHow.asp">https://web.archive.org/web/20020814065623/http://www.ztrace.com:80/zTraceHow.asp</a>                                            |
| 1023        | zTrace – About zTrace page:<br><a href="https://web.archive.org/web/20020604025540/http://www.ztrace.com:80/AboutzTrace.asp">https://web.archive.org/web/20020604025540/http://www.ztrace.com:80/AboutzTrace.asp</a>                                            |
| 1024        | zTrace – Press Release re zTrace Security Suite:<br><a href="https://web.archive.org/web/20021019100311/http://www.ztrace.com/pr_releases/HPEducational.pdf">https://web.archive.org/web/20021019100311/http://www.ztrace.com/pr_releases/HPEducational.pdf</a> |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

| Exhibit No. | Description of Document                                                                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1025        | zTrace – 2003 Press Releases page:<br><a href="https://web.archive.org/web/20030820024638/http://www.ztrace.com:80/PressReleases.asp">https://web.archive.org/web/20030820024638/http://www.ztrace.com:80/PressReleases.asp</a>                                 |
| 1026        | zTrace – Press Release re zControl:<br><a href="https://web.archive.org/web/20040518054736/http://www.ztrace.com/pr_releases/zControl.pdf">https://web.archive.org/web/20040518054736/http://www.ztrace.com/pr_releases/zControl.pdf</a>                        |
| 1027        | zTrace – 2004 Press Releases page:<br><a href="https://web.archive.org/web/20040226194817/http://ztrace.com/PressReleases.asp">https://web.archive.org/web/20040226194817/http://ztrace.com/PressReleases.asp</a>                                               |
| 1028        | zTrace – Press Release for Yale University and zTrace Partnership:<br><a href="https://web.archive.org/web/20040531010618/http://www.ztrace.com/pr_releases/Yale.pdf">https://web.archive.org/web/20040531010618/http://www.ztrace.com/pr_releases/Yale.pdf</a> |
| 1029        | U.S. Patent Application Publication No. 2002/0045437 A1 issued to Alexander Kesler (filed Aug. 16, 2001, issued Apr. 18, 2002) (“Kesler”)                                                                                                                       |
| 1030        | U.S. Patent No. 5,748,084 issued to Jeremy M. Isikoff (filed Nov. 18, 1996, issued May 5, 1998) (“Isikoff”)                                                                                                                                                     |
| 1031        | U.S. Patent Application Publication No. 2003/0051090 A1 issued to William B. Bonnett et al. (filed Jul. 17, 2002, issued Mar. 13, 2003) (“Bonnett”)                                                                                                             |
| 1032        | U.S. Patent No. 6,542,979 B1 issued to Donald J. Eckardt (filed Mar. 31, 1999, issued Apr. 1, 2003) (“Eckardt”)                                                                                                                                                 |
| 1033        | Affidavit of Nathaniel E Frank-White, dated October 17, 2023                                                                                                                                                                                                    |
| 1034        | Declaration of Dr. Mary K. Bolin                                                                                                                                                                                                                                |
| 1035        | Excerpts from 386™ DX Programmer’s Reference Manual                                                                                                                                                                                                             |
| 1036        | Ex. 5 to Softex’s Infringement Contentions in the <i>Softex LLC v. Absolute Software Corporation et al.</i> , No. 1:22-cv-01308 (W.D. Tex.)                                                                                                                     |
| 1037        | Excerpts from Newton’s Telecom Dictionary (17th ed. 2001)                                                                                                                                                                                                       |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

| <b>Exhibit No.</b> | <b>Description of Document</b>                                                                                                                                                                                                                   |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1038</b>        | Excerpts from Terry William Ogletree et al., Windows XP Unleashed (2002)                                                                                                                                                                         |
| <b>1039</b>        | U.S. Patent No. 6,300,863 issued to Christian Cotichini et al. (filed Mar. 24, 1998, issued Oct. 9, 2001) (“Cotichini”)                                                                                                                          |
| <b>1040</b>        | U.S. Patent No. 10,257,551 B2 issued to Leslie L. Grandy et al. (filed Dec. 12, 2016, issued Apr. 9, 2019) (“Grandy”)                                                                                                                            |
| <b>1041</b>        | U.S. Patent No. 6,775,828 B2 issued to David Feinleib et al. (filed July 19, 1999, issued Aug. 10, 2004) (“Feinleib”)                                                                                                                            |
| <b>1042</b>        | U.S. Patent No. 7,716,719 B2 issued to Victor Kouznetsov et al. (filed Apr. 21, 2005, issued May 11, 2010) (“Kouznetsov”)                                                                                                                        |
| <b>1043</b>        | U.S. Patent No. 8,983,896 B2 issued to Tim A. von Kaenel et al. (filed July 7, 2011, issued Mar. 17, 2015) (“von Kaenel”)                                                                                                                        |
| <b>1044</b>        | Excerpts from Douglas Comer, Operating System Design, The Xinu Approach, Linksys Version (2012) (“Comer”)                                                                                                                                        |
| <b>1045</b>        | Herb Goronkin & Yang Yang, <i>High-Performance Emerging Solid-State Memory Technologies</i> , MRS Bulletin, 806-813 (Nov. 2004) (“Goronkin”)                                                                                                     |
| <b>1046</b>        | Roberto Bez et al., <i>Introduction to Flash Memory</i> , Proceedings of the IEEE, 91(4):489-502 (Apr. 2003) (“Bez”)                                                                                                                             |
| <b>1047</b>        | U.S. Patent No. 5,852,306 issued to Leonard Forbes (filed Jan. 29, 1997, issued Dec. 22, 1998) (“Forbes”)                                                                                                                                        |
| <b>1048</b>        | Excerpts from Andrew S. Tanenbaum, Operating Systems: Design and Implementation (1987)                                                                                                                                                           |
| <b>1049</b>        | U.S. Patent No. 5,537,540 issued to Craig A. Miller et al. (filed Sept. 30, 1994, issued July 16, 1996) (“Miller”)                                                                                                                               |
| <b>1050</b>        | U.S. Patent No. 6,725,178 B2 issued to Richard W. Cheston et al. (filed Jan. 15, 2002, issued Apr. 20, 2004) (“Cheston”)                                                                                                                         |
| <b>1051</b>        | U.S. Patent Application Publication No. US 2002/0188837 A1 issued to Richard Alan Dayan et al. (filed June 7, 2001, publication date Dec. 12, 2002) (“Dayan”)                                                                                    |
| <b>1052</b>        | zTrace – Protect, Monitor, Recover:<br><a href="https://web.archive.org/web/20030811214545/http://www.ztrace.com:80/home_ie.asp">https://web.archive.org/web/20030811214545/http://www.ztrace.com:80/home_ie.asp</a>                             |
| <b>1053</b>        | zTrace – zControl Maintains data privacy after computer loss:<br><a href="https://web.archive.org/web/20030811223300/http://www.ztrace.com:80/zControl.asp">https://web.archive.org/web/20030811223300/http://www.ztrace.com:80/zControl.asp</a> |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

| <b>Exhibit No.</b> | <b>Description of Document</b>                                                                                                                                                                                                                                                                                                        |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1054</b>        | Edward C. Baig, <i>Unlock the secrets of security for your laptop</i> , USA Today (April 9, 2002),<br><a href="https://web.archive.org/web/20060504120338/http://www.usatoday.com:80/tech/columnist/2002/04/10/baig.htm">https://web.archive.org/web/20060504120338/http://www.usatoday.com:80/tech/columnist/2002/04/10/baig.htm</a> |
| <b>1055</b>        | Yahoo Internet Life Magazine, <i>URL Guide</i> , zTrace.com (July 2002),<br><a href="https://web.archive.org/web/20021025034410/http://www.ztrace.com/sites/yahoo50/yil.com.html">https://web.archive.org/web/20021025034410/http://www.ztrace.com/sites/yahoo50/yil.com.html</a>                                                     |
| <b>1056</b>        | Plaintiff's Objections and Responses to Absolute's Individual Interrogatories to Plaintiff (Nos. 1-8), served on September 25, 2023 in <i>Softex LLC v. Absolute Software Corp.</i> , No. 1:22-cv-01308 (W.D. Tex.)                                                                                                                   |
| <b>1057</b>        | Summons in a Civil Action Return of Service, filed in <i>Softex LLC v. Absolute Software Corp.</i> , No. 1:22-cv-01308, D.I. 8 (W.D. Tex. Dec. 19, 2022)                                                                                                                                                                              |
| <b>1058</b>        | Affidavit of Nathaniel E Frank-White, dated November 16, 2023                                                                                                                                                                                                                                                                         |

**I. MANDATORY NOTICES UNDER § 42.8(A)(1)**

**A. Related Matters under § 42.8(b)(2)**

The '649 patent is the subject of the following pending litigation involving Petitioner: *Softex LLC v. Absolute Software Corp.*, No. 1:22-cv-01308-DAE (W.D. Tex.). Petitioners were served with the Complaint in that action on December 16, 2022. (EX1057.)

The '649 patent is also the subject of the following litigations:

- *Softex LLC v. Dell Technologies Inc.*, No. 1:22-cv-01309-DAE (W.D. Tex.);
- *Softex LLC v. HP Inc.*, No. 1:22-cv-01311-DAE (W.D. Tex.);
- *Softex LLC v. Lenovo (Shanghai) Electronics Technology Co.*, No. 5:23-CV-90-BO (E.D.N.C.) (stayed).

Microsoft Corporation's ("Microsoft") products are accused in these three cases, but Microsoft is not a named party. On July 11, 2023, Microsoft filed an IPR petition challenging claims 1-25 of the '649 patent, pending as IPR2023-01185. Microsoft has no connection to the present Petition.

**B. Real Party-In-Interest under § 42.8(b)(1)**

Absolute Software Corporation and Absolute Software, Inc. are the real parties-in-interest (RPIs) to this IPR petition.

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

Dell, HP, Lenovo, and Microsoft are not RPIs in-fact to the present Petition. These parties did not request, direct, fund, or control the development of this Petition. Nor were they aware of the existence of this Petition until it was filed. Petitioners also challenge only the claims that Patent Owner (PO) asserts against their software (*i.e.*, claims 1, 7, 9, and 15) and omits claims 3 and 10—the claims only asserted against Microsoft’s products in the HP, Dell, and Lenovo cases.

While Petitioners have indemnified Dell, HP, and Lenovo with respect to challenged claims in their respective cases, it is Petitioners—not Dell, HP, or Lenovo—that provided outside counsel and funds to litigate these claims under the agreements. Indemnification does not *per se* establish an RPI. For example, in *Ventex* the Board found an indemnitee was an RPI only where that party *also* had an exclusive manufacturing agreement with the petitioner. *See Ventex Co. v. Columbia Sportswear N. Am., Inc.*, IPR2017-00651, Paper 152 at 10 (P.T.A.B. Jan. 24, 2019) (precedential). No exclusive manufacturing agreement exists between Petitioners and any of HP, Dell, or Lenovo.

Finally, RPI concerns are typically raised over concerns about the § 315(b) statutory deadline that is not present here. PO served Petitioners, Dell, HP, and Lenovo on December 16, 2022. *See SharkNinja Operating LLC v. iRobot Corp.*, IPR2020-00734, Paper 11 at 18 (PTAB Oct. 6, 2020) (precedential) (“[W]e

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

determine that we need not address whether [a party] is an unnamed RPI because, even if it were, it would not create a time bar or estoppel under 35 U.S.C. § 315.”).

**C. Lead and Back-Up Counsel under § 42.8(b)(3)**

Petitioners provide the following designation of counsel.

| LEAD COUNSEL                                                                                                                                                                                                   | BACK-UP COUNSEL                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Heidi L. Keefe<br>(Reg. No. 40,673)<br>hkeefe@cooley.com<br><br>COOLEY LLP<br>ATTN: Patent Group<br>1299 Pennsylvania Ave. NW, Suite 700<br>Washington, DC 20004<br>Tel: (650) 843-5001<br>Fax: (650) 849-7400 | Orion Armon<br>(Reg. No. 65,421)<br>oarmon@cooley.com<br><br>COOLEY LLP<br>ATTN: Patent Group<br>1299 Pennsylvania Ave. NW, Suite 700<br>Washington, DC 20004<br>Tel: (720) 566-4119<br>Fax: (720) 566-4099                  |
|                                                                                                                                                                                                                | Jennifer Volk-Fortier<br>(Reg. No. 62,305)<br>jvolkfortier@cooley.com<br><br>COOLEY LLP<br>ATTN: Patent Group<br>1299 Pennsylvania Ave. NW, Suite 700<br>Washington D.C. 20004<br>Tel: (703) 456-8575<br>Fax: (703) 456-8100 |
|                                                                                                                                                                                                                | Reuben Chen<br>( <i>Pro hac vice</i> application to be filed)<br>rchen@cooley.com<br><br>COOLEY LLP<br>ATTN: Patent Group<br>1299 Pennsylvania Avenue NW<br>Suite 700                                                        |

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

| LEAD COUNSEL | BACK-UP COUNSEL                                                                                                                                                                                                        |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | Washington D.C. 20004<br>Tel: (650) 843-5480<br>Fax: (650) 849-7400                                                                                                                                                    |
|              | Dustin M. Knight<br>(Reg. No. 76,239)<br>dknight@cooley.com<br><br>COOLEY LLP<br>ATTN: Patent Group<br>1299 Pennsylvania Avenue NW<br>Suite 700<br>Washington D.C. 20004<br>Tel: (703) 456-8024<br>Fax: (703) 456-8100 |

**D. Service Information**

This Petition is being served by Federal Express to the attorney of record for the '649 patent, GEORGIOS GEORGAKIS, 138358 - G+J Softex Temp, 4301 W WILLIAM CANNON DR, STE B150 PMB 200, AUSTIN, TX 78749-1487, in compliance with 37 C.F.R. § 42.8(b)(4). This Petition is also being served on litigation counsel identified in the Certificate of Service. Petitioners consent to electronic service at the addresses provided above for lead and back-up counsel.

**E. Power of Attorney**

Filed concurrently per 37 C.F.R. § 42.10(b).

**II. FEE PAYMENT**

Petitioners request review of four claims, with a \$41,500 payment.

### **III. REQUIREMENTS UNDER §§ 42.104 AND 42.108 AND CONSIDERATIONS UNDER §§ 314(A) AND 325(D)**

#### **A. Standing**

Petitioners certify that the '649 patent is available for IPR and that Petitioners are not barred or otherwise estopped.

#### **B. Identification of Challenge**

Petitioner requests institution of IPR based on the following grounds:

| <b>Ground</b> | <b>Claim(s)</b> | <b>Basis for Challenge</b>                    |
|---------------|-----------------|-----------------------------------------------|
| 1             | 1, 7, 9, 15     | zTrace in view of Kesler, Isikoff and Bonnett |
| 2             | 1, 7, 9, 15     | zTrace in view of Kesler, Isikoff and Eckardt |

Submitted herewith is a Declaration of Dr. Nathaniel Polish, Ph.D. (EX1003), a qualified expert. EX1003, ¶¶ 1-11, Ex. A.

#### **C. §§ 314(a) and 325(d)**

Petitioners respectfully submit that no basis exists under either § 314(a) or § 325(d) for discretionary denial of this Petition. Petitioners reserve their rights to respond to any discretionary denial arguments later presented by PO.

**§ 314(a)**: With respect to § 314(a), Petitioners have not previously filed an IPR petition against the '649 patent. No claim construction or other substantive rulings have issued in the pending litigation. A trial date has not been set. Petitioners hereby provide a *Sotera* stipulation that, in the event of IPR institution, Petitioners

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

will not pursue in the district court any grounds of invalidity against the challenged claims that were raised or reasonably could have been raised in IPR. While Microsoft filed an IPR on July 23, 2023 this is not a parallel IPR petition under the *General Plastic* factors discussed below.

**Factor #1:** Petitioners are different than Microsoft and did not cooperate with Microsoft in the development of this Petition. Nor were Petitioners involved in any capacity in the funding, preparation, or filing of Microsoft’s petition in IPR2023-01185—Petitioners were not aware of that petition until after it was filed. Nor have Microsoft and Petitioners indirectly cooperated through HP, Dell, or Lenovo. Each of these entities are separately and independently indemnified by Microsoft because PO accused Microsoft’s product of infringing a broader set of claims to the ’649 patent than those challenged here. “The fact that a different petitioner is involved in this proceeding weighs especially heavily against a discretionary denial.” *Toshiba Am. Info. Sys., Inc. v. Wallelex Microelectronics Ltd.*, IPR2018-01538, Paper 11 at 20 (PTAB Mar. 5, 2019).

**Factor #3:** This Petition does not benefit from a “roadmap” because the Board has not issued an institution decision in IPR2023-01185. *See Code200 v. Bright Data Ltd.*, IPR2022-00861, Paper 18 at 5 (PTAB Aug. 23, 2022) (precedential). Nor is the POPR in IPR2023-01185 a “roadmap” for this Petition. The POPR focuses

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

primarily on procedural and 314(a) matters that are irrelevant to the substantive issues in this Petition. The substantive arguments PO raises are directed to different art and limited to the “automatically sending identifying information” and “accepting a notification... from the security service” limitations that are disclosed by the combination of zTrace, Kesler and Isikoff in this petition.

**Factors # 6, 7:** The Board’s resources are well-applied by considering this Petition. Petitioners assert substantially different prior art grounds than those present in IPR2023-01185 against fewer claims, resulting in a more streamlined proceeding. *W. Digit. Corp. v. SPEX Techs., Inc.*, IPR2018-00084, Paper 14 at 17 (PTAB Apr. 25, 2018). Petitioners also present a strong primary reference—zTrace—that discloses or suggests every limitation of the Challenged Claims.<sup>1</sup>

**Factors # 2, 4, 5:** As Microsoft and Petitioners differ, “the second through fifth factors bear little relevance.” *Toshiba*, IPR2018-01538, Paper 11 at 21.

**§ 325(d):** The Board assesses § 325(d) issues under the two-part *Advanced Bionics* framework: (1) whether the same or substantially the same art was previously presented to the Office and if so (2) whether Petitioners have

---

<sup>1</sup> Petitioners include secondary references in **Ground 1** and **Ground 2** to reinforce the suggested disclosures in zTrace.

demonstrated that the Examiner erred in a manner material to the patentability of challenged claims. Part (1) does not apply to **zTrace** (EX1004-EX1028 and EX1052-EX1053), relied upon in **Grounds 1** and **2**, or **Eckardt** (EX1032), relied upon in **Ground 2**, because neither reference was considered during prosecution of the '649 patent, and zTrace's and Eckardt's disclosures are not substantially the same as art that was previously presented to the Office.

As to parts (1) and (2), Kesler, Isikoff, and Bonnett were previously cited in an IDS during prosecution but were not the basis for any Office Action related to the presently asserted claims. As demonstrated below, the Examiner materially erred in allowing the claims of the '649 to issue over Bonnett, Kesler and Isikoff.

**Bonnett:** **Ground 1** relies on this reference for its non-volatile memory disclosures related to limitations 1[d]-1[g], and in particular for storing programs in a hidden system area. The applicant cited Bonnett in an IDS that was submitted before the Examiner issued the first office action. EX1002, 372. The Examiner did not rely on Bonnett as a ground for rejection in the first office action. At the time, the claims recited that the “application component” was part of the “*changeable* area in the nonvolatile storage device,” whereas the issued claims now recite that the “the

security application utilizes code residing at least partially in the *system* area,” so the pending claims had materially different scope at that time. EX1002, 359, 335.<sup>2</sup>

After this first office action, the applicant canceled all claims and submitted a new set that resulted in the issued claims. EX1002, 305-317. There is no indication from the Examiner’s search results that he re-examined Bonnett and other references cited prior to the first office action to determine if they rendered the new claim set, with a different claim scope, obvious. EX1002, 286-293. This was an error, as Bonnett discloses these later, issued limitations. *See Hum Indus. Tech., Inc. v. Amsted Rail Co.*, IPR2023-00540, Paper 10 at 44 (PTAB Aug. 11, 2023) (“*Hum Indus. Tech.*”) (error where examiner “did not sufficiently evaluate or appreciate the relevance” of a reference’s teachings at the time of review).

**Kesler:** Kesler was cited in an IDS in February 2010 and the examiner initialed Kesler as part of the final office action that issued in April 2010. EX1002, 294-295, 292-293. Two years later PO added limitation 1[c][iii] (related to “periodically communicating” with the server) to the claims. EX1002, 103. Based on this amendment, the claims were allowed.

Kesler discloses “periodically communicating” as discussed below. There is no indication in the Examiner’s search results that he re-examined Kesler to

---

<sup>2</sup> Emphasis added unless noted otherwise.

determine if it taught the newly added limitation. If he had, the application would not have moved to allowance. This was a material error. *See Hum Indus. Tech.*, Paper 10 at 44. In addition, no arguments were made for this limitation during prosecution, rendering the arguments in this Petition related to limitation 1[c][iii] new. Kesler is related to zTrace, but it omits many disclosures provided by the zTrace art (described herein below), so Kesler and zTrace are non-cumulative.

**Isikoff:** Isikoff was cited in an IDS on November 6, 2010 and the examiner initialed Isikoff as part of the non-final office action that issued in December 2011. EX1002, 212, 184. Isikoff discloses “disabling” as discussed below. The claims at the time recited a similar “disabling” feature but the examiner relied on another prior art reference in its non-final office action. No arguments were made about this limitation during prosecution, rendering the arguments in this Petition related to limitations 1[c][iv] and 1[c][v] new.

#### **IV. OVERVIEW OF THE '649 PATENT**

The '649 patent, which purports priority to a provisional application filed on August 23, 2003<sup>3</sup>, describes an “electronic device security and tracking system and

---

<sup>3</sup> Petitioners assume this priority date without waiving the right to challenge the date in another proceeding.

method” (“ESTSM”) that “includes a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with [a] stolen electronic device.” EX1001, 1:36-2:15. More details regarding this patent are included in the declaration. EX1003, ¶¶36-40.

The Challenged Claims are appended to this Petition as **Appendix A**.

## **V. LEVEL OF ORDINARY SKILL IN THE ART**

A person of ordinary skill in the art (“POSITA”) as of August 23, 2003 would have possessed an undergraduate degree in computer science (or related field) and one to two years of experience developing security-related software for mobile devices and would further have familiarity with non-volatile memories. Additional education could compensate for less practical experience. Conversely, additional practical experience could compensate for less education. EX1003, ¶¶13-18.

## **VI. CLAIM CONSTRUCTION**

In district court, the parties agreed that the terms in the ’649 patent should take on their plain and ordinary meaning, subject to further interpretation depending on how the parties’ infringement and invalidity theories evolve throughout the case. The plain and ordinary meaning should also apply in this proceeding. The Board need not construe any claim term to decide the validity of the challenged claims in light of the Proposed Grounds. EX1003, ¶27.

## VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

### A. Prior Art

#### 1. zTrace [EX1004-EX1028, EX1052-EX1053]

zTrace is a collection of archive.org-verified webpages from the zTrace.com website, with capture dates ranging from April 5, 2002 to August 20, 2003 [EX1004-EX1025, EX1052-EX1053] and additionally from February 26, 2004 to May 31, 2004 [EX1026-EX1028], that describe different cyber security products and services offered by zTrace Technologies. EX1033; EX1034, ¶¶18-127, 159-166; EX1058; EX1003, ¶¶43-59. The later webpages identify content that was publicly available prior to the assumed August 23, 2003 priority date for the '649 patent.

EX1026 is a press release for a zTrace Technology product called “zControl” that is dated January 15, 2003 (excerpted, annotated and shown below) but it has an archive.org capture date of May 18, 2004. EX1033, 53-54.



#### zControl Released

Boston, MA, January 15, 2003 - zTrace Technologies today announces the release of zControl, the latest security software in the zTrace

EX1025 captured the zTrace.com press release page on August 20, 2003 (excerpted, annotated and shown below) and it lists the same zControl press release with the

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

same January 15, 2003 date, confirming that this press release [EX1026] was publicly available at least three days prior to August 23, 2003. EX1033, 16.

### Press Releases



**zTrace Participates in SoftwareToGo rollout in CompUSA 225 stores**  
Boston, MA, August 7, 2003



**zTrace Technologies Partners with Xylos to Track Down Stolen PCs and Recover Information After Theft in Belgium and Luxembourg**  
Boston, MA, August 1, 2003



**ZCONTROL Released**  
Boston, MA, January 15, 2003

See also EX1034, ¶¶86, 88, Attachment RA (at 83) (showing a pre-August 2003 creation date for the pdf document). The content in this press release was also included in an August 11, 2003 capture of the zTrace.com webpage for zControl [EX1053]; therefore, all invalidity arguments set forth below are supported by webpages with capture dates that pre-date August 23, 2003.

EX1028 is a press release for a Yale University collaboration dated August 20, 2003 (excerpted, annotation and shown below) but it has an archive.org capture date of May 31, 2004. EX1033, 51-52.



#### Yale University Selects zTrace to Provide Laptop Protection to Students

Boston, MA, **August 20, 2003** - zTrace Technologies announces its partnership with Yale University to provide zTrace Gold and zControl, its

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

EX1027 captured the zTrace.com press release page on February 26, 2004 and it lists the same Yale University collaboration press release with the same August 20, 2003 date. EX1033, 14.

## Press Releases



**Yale University Selects zTrace to Provide Laptop Protection to Students**  
Boston, MA, **August 20, 2003**

*See also* EX1034, ¶98, Attachment TA (at 89) (showing a pre-August 2003 creation date for the pdf document).

Additional details regarding the public availability of EX1026-EX1028 (and EX1004-EX1025, EX1052-EX1053) are included in the Internet Archive affidavits **[EX1033 & EX1058]**, Dr. Bolin's declaration **[EX1034]** and Dr. Polish's declaration **[EX1003]**. Each webpage cited in a Proposed Ground as an invalidating reference qualifies as a publication and prior art under 35 U.S.C. §§ 102(a) or (b). *See Sandoz Inc. v. Abbvie Biotechnology Ltd.*, IPR2018-00156, Paper 11 at 8-13 (PTAB June 5, 2018) (informative) (finding that a webpage from the Wayback Machine, a declaration from the office manager of the Internet Archive including the site's archival records, and expert testimony asserting its public accessibility was sufficient for instituting an *inter partes* review"); *see also Hulu LLC v. Sound View*

*Innovations LLC*, IPR2018-01039, Paper 29 at 18 (PTAB Dec. 20, 2019)  
(precedential).

The webpages describe a service known as zTrace™. The zTrace™ service “aids in the recovery of stolen or missing computers, protects sensitive data in case of unauthorized access and effectively monitors hardware and software assets for tracking.” EX1005. Laptop owners download protective software applications from zTrace onto their laptops via a zServer. EX1019, 2-3; *see also* EX1004 (excerpted above at right).



A variant of zTrace called “zTrace Gold” is “an invisible software security application that traces the location of missing laptops for recovery.” EX1007. Another zTrace product called “zControl” is also “an invisible software application” that “provides automated control of a computer’s data even AFTER loss has occurred.” EX1013. Other zTrace products include “zAsset Track,” “Pass” and “zEncrypt.” EX1005.

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

In use, zTrace Gold is installed on the laptop's hard drive. EX1007 (shown at left). With each Internet connection, zTrace Gold causes the laptop to communicate



with the zServer to determine whether the laptop has been reported lost or stolen. *Id.* If the zServer responds that the laptop is reported lost or stolen, zTrace Gold “reports its own location” to the zServer so the zTrace service can start the recovery process. *Id.*

The registered owner of the laptop can utilize zControl to protect and recover sensitive information stored on the laptop while the recovery process is underway. zTrace provides a “zControl web-based user interface” that allows owners to “order[] the remote and invisible deletion of files, recovery of data to the zServer and remote encryption of data.” EX1026; EX1053; EX1013. zTrace touts that “[t]here are no icons, files, directories, sounds or ANYTHING visible on the computer, providing total invisibility to the user.” EX1005 (excerpted and shown below).

**"You can't steal what you can't see."**  
**Alexander Kesler, Founder and President of zTrace**

zTrace discloses or suggests each of the limitations in the Challenged Claims.

## 2. Kesler [EX1029]

Kesler published on April 18, 2002 and is prior art under 35 U.S.C. § 102(b). Notably, the sole inventor of this publication—Alexander Kesler—is also the creator of the zTrace™ technology described above. Kesler, cover at (76); EX1005. In fact, Kesler loosely references the “zTrace” technology in one of its embodiments. Kesler, [0035] (“the client tracing software 32 includes three main modules: zAgent 34, zCore 36, and zTrace 38”). Kesler describes a system and service for tracking lost mobile devices. Kesler, FIG. 1, [0015]-[0017]. For example, as shown below in Figure 1, Kesler describes a registration process that ends in the mobile device owner installing tracing software on the hard drive of her mobile device. Kesler, [0015], [0024]-[0025].

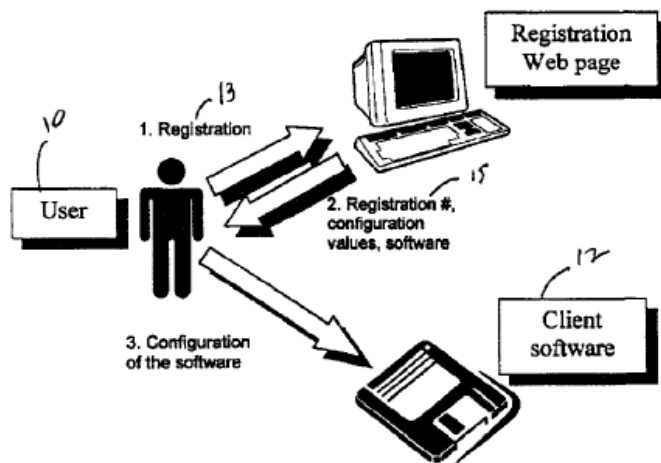


Figure 1

“[T]he software will download invisibly and install itself, which significantly reduces the opportunity for tampering.” Kesler, [0017]. Kesler explains that “[e]ach

time the user connects the computer to the Internet, the tracing software connects to a tracing server 14 through the Internet.” Kesler, [0015]. If the mobile device is reported stolen, the tracing server notifies the tracing software, as shown below in Figure 2. Kesler, [0017].

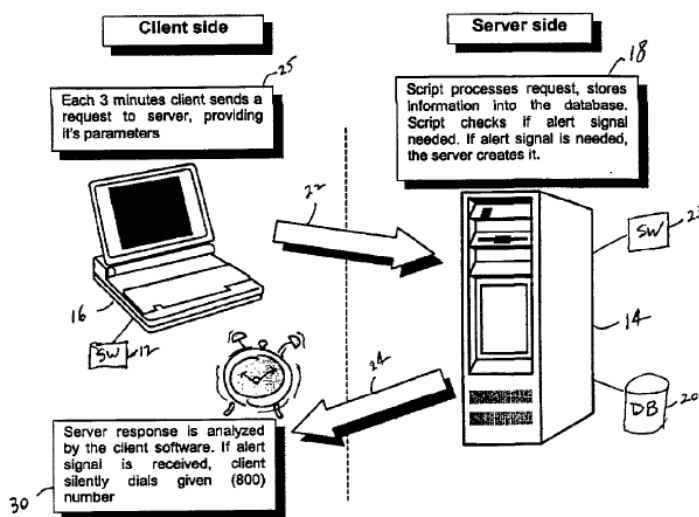


Figure 2

Kesler does not disclose all of the functionalities of zTrace discussed in this Petition. Kesler provides certain disclosures not expressly taught in zTrace. For example, Kesler discloses that part of its tracing software is “installed onto track zero” of the hard drive, which is known to be a hidden track. Kesler, [0017]. Kesler also expressly discloses that its tracing software sends identifying information, such as an “assigned registration number,” to the tracing server as part of its communications. Kesler, [0025]-[0026]. Kesler further discloses that the tracing

software can check for an Internet connection and contact the tracing server at predefined intervals, for example, every 20 minutes. Kesler, [0032]-[0033].

Kesler is relied on here as a secondary reference to supplement the disclosures of zTrace. A POSITA would have looked to Kesler as an informative reference about the zTrace™ functionality. EX1003, ¶¶60-64.

### 3. Isikoff [EX1030]

Isikoff published on May 5, 1998 and is prior art under 35 U.S.C. § 102(b). Isikoff discloses certain “disabling” functionality recited in the Challenged Claims.

Isikoff discloses a laptop security and tracking scheme similar to zTrace and Kesler. Isikoff, Abstract (“An object tracking, communication, and management system for a laptop computer or similar device, wherein a beacon or transceiver in the computer implements...

device recovery steps”), FIG. 1 (shown at right). The laptop in Isikoff includes a beacon capable of receiving “low level control codes” that instruct the beacon to

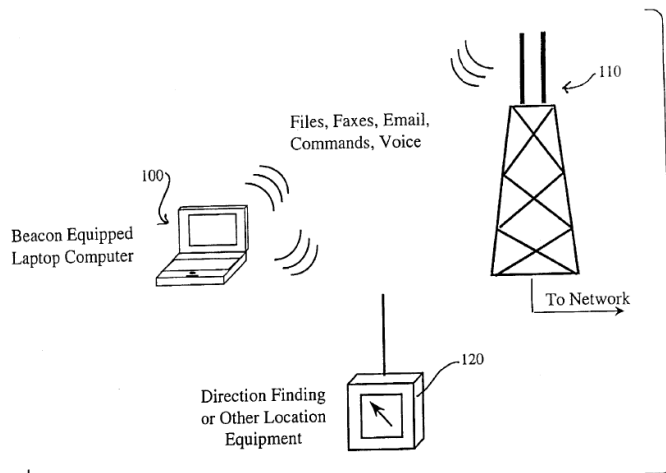


Figure 1

“implement at least some of the security features of the device... includ[ing] the disabling or interruption of power to all or to specific parts of the computer,... or the

erasure of the hard drive.” Isikoff, 5:59-6:5; *see id.*, Abstract, 3:46-53, 4:3-14, 6:17-30.

#### 4. Bonnett [EX1031]

Bonnett published on March 13, 2003 and is prior art under 35 U.S.C. § 102(a). It discloses a method for securing software programs in memory, such as “a NAND flash memory,” so that users cannot “delet[e] or corrupt[.]” the programs. Bonnett, [0011], [0031]. The memory in Bonnett has an “open partition” and a “hidden partition.” Bonnett, [0007], [0032]-[0037]. The open partition is “accessible to the user” and stores “media files [and] data files[.]” Bonnett, [0036]. The hidden partition is “substantially free from access by a user” and stores the protected program. Bonnett, [0032], [0037].

Bonnett is relied on to disclose the “**non-volatile memory**” limitations of independent claims 1 and 9 under **Ground 1**.

#### 5. Eckardt [EX1032]

Eckardt published on April 1, 2003 and is prior art under 35 U.S.C. § 102(a). It explains that “hard disks... are often ‘partitioned’ into multiple logical subdivisions,” (Eckardt, 1:10-16), and that a partition could be “hidden” such that the partition and its contents “cannot be read or modified,” (*id.*, 1:35-46, 4:50-59).

Eckardt is relied on to disclose the “**non-volatile memory**” limitations of independent claims 1 and 9 under **Ground 2**.

**B. Ground 1: Claims 1, 7, 9 and 15 are rendered obvious by zTrace in view of Kesler, Isikoff and Bonnett**

**1. Independent claim 1**

The preamble recites “[a] **mobile electronic device, comprising**” the components set forth in the subsequent limitations. zTrace discloses implementing its security software in “Laptop Computers,” which are “**mobile electronic device[s]**.” EX1019, 2 (“zTrace™ will run on Desktop and Laptop Computers”); EX1006.

**(a) Limitation 1[a]**

This limitation is disclosed by zTrace. zTrace “run[s] on Desktop and Laptop Computers with Windows XP, 2000, ME, 98[,] 386 DX or higher, 16 MB RAM, 2M HD space.” EX1019, 2. The “386 DX” is a processor produced by Intel. EX1035, 1 (“386™ DX Programmer’s Reference Manual”); EX1003, ¶¶74-75.

**(b) Limitation 1[b]**

This limitation is disclosed or suggested by zTrace. EX1003, ¶¶76-79. zTrace “run[s] on Desktop and Laptop Computers with Windows XP, 2000, ME, 98[,] 386 DX or higher, 16 MB RAM, 2M HD space.” EX1019, 2. The “2M HD” refers to the program requiring 2 megabytes of hard drive. EX1003, ¶76. Hard drives are known “**non-transitory machine-readable storage media.**” *See* EX1001, 35:40-42

(confirming that “[s]torage devices such as memory, disk drives, etc. may also be referred to as non-transitory machine-readable storage media”).

A hard drive is “**responsive to the processor**,” as the hard drive stores data utilized by the processor. EX1003, ¶77. For example, the 386™ DX Programmer’s Reference Manual explains that the processor uses “paging” as a form of memory management that involves storing and retrieving data from the hard disk. *See* EX1035, 1-1 (“The 386 DX microprocessor includes... paging, a form of memory management which provides access to data structures larger than the available memory space by keeping them partly in memory and partly on disk”), 2-1, 2-2, 5-1, 5-2, 5-10, 5-11, 5-17, 5-18, 5-21, 5-22, 6-6, 6-22, 9-3, 10-5. Because the laptop in zTrace includes the 386 DX processor, it is understood that the processor would use this well-known paging technique to retrieve data from the laptop’s hard drive, resulting in the hard drive being “**responsive to the processor**.” EX1003, ¶¶78-79 (also explaining that the zTrace applications in the hard drive are executed by the 386 DX processor, further resulting in the hard drive being “**responsive to the processor**”).

**(c) Limitation 1[c]**

As a preliminary matter, the term “**a**” is typically interpreted to mean “one or more” absent a clear disclaimer in the specification or prosecution history. *See*

*Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342-43 (Fed. Cir. 2008) (“[T]his court has repeatedly emphasized that an indefinite article ‘a’ or ‘an’ in patent parlance carried the meaning of ‘one or more’ in open-ended claims containing the transitional phrase ‘comprising’” unless the patentee “‘evince a clear intent’ to limit ‘a’ or ‘an’ to ‘one’.” (citing *KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1356 (Fed. Cir. 2000))). Thus, the plain and ordinary meaning of “**a security application**” is one or more security applications. *See also* EX1001, 2:53-57 (identifying “ESTSM application components”), 3:6-8, 3:32-38, 17:11-13, 17:21-28, 17:39-61, 19:13-16, 23:4-5, 26:11-17 (“the ESTSM application component consists of two sets of programs”), 26:57-7:6; EX1003, ¶80.

zTrace discloses a suite of software applications, including the zTrace Gold application and the zControl application. EX1004; EX1005. Each application is a “**security application.**” These “software applications [] aid[] in the recovery of stolen or missing computers, [and] protect[] sensitive data in case of unauthorized access,” as will be discussed in the next sections (i.e., “**the security application is operable to perform operations comprising**”). EX1005; EX1003, ¶¶81-82.

zTrace discloses that “zTrace Gold is installed on the laptop’s hard drive[.]” EX1007; EX1006. Therefore, at least this “**security application**” is “**in at least one of the non-transitory machine-readable storage media.**” EX1003, ¶83.

zTrace is silent with respect to where the zControl application is installed. zTrace, however, only identifies two storage media capable of storing this application—a RAM and a hard drive—and only the hard drive provides a non-volatile storage solution. *See* EX1019, 2 (zTrace “run[s] on Desktop and Laptop Computers with Windows XP, 2000, ME, 98[, ] 386 DX or higher, 16 MB RAM, 2M HD space.”); EX1003, ¶84 (explaining that RAM is a volatile memory that only temporarily stores data but the hard drive is a non-volatile memory that provides persistent storage after the laptop is turned off). Thus, a POSITA would have understood, or found it obvious, that zControl is installed on the laptop’s hard drive, as this is the most logical location for long-term storage of the zControl application on the laptop. EX1003, ¶¶84-85, 87, 90.

Also, as will be discussed in more detail with respect to limitations 1[e] and 1[f], installing the zControl application on the hard drive would allow it to remain “invisible” to the normal user, as it was well known that hard drives include secure or hidden areas for this purpose. *See, e.g.*, EX1013 (touting zControl as “an invisible software application”); EX1007; EX1003, ¶¶85-92 (citing Kesler, [0017]; Eckardt, 1:10-49; Cotichini, FIG. 20, 29:24-38).

For at least these reasons, zTrace suggests or renders obvious that the zControl “**security application**” is “**in at least one of the non-transitory machine-readable**

**storage media.”**

To the extent the Board interprets “**a security application**” to mean a single application, zTrace would still render this limitation obvious. EX1003, ¶¶93-100. zTrace explains that its applications “collectively” “provide the optimum wrap around security solution” for its customers. EX1005. The “suite affords single installation of the zTRACE circle of complete mobile care-integrated software for tracing and recovery, [and] data protection[.]” *Id.* zTrace therefore refers to its applications as a single software solution that is provided in a single installation. *Id.* Certain zTrace disclosures also refer to the applications as a single “program.” *see also* EX1019, 3 (Q: “Can I remove zTrace™?” A: “A subscriber can remove *the program* from his/her computer using a personalized password”); EX1003, ¶93.

With respect to the zTrace Gold and zControl applications specifically, zTrace created a “zSecurity Pack” in early 2003 that included only these two applications. EX1052; EX1026. zTrace’s press release explains:

zControl is the perfect complement to our zTrace Gold product. While zTrace Gold provides a stealth solution for protecting and retrieving your hardware, zControl provides a stealth solution for protecting and retrieving your valuable data. The two products, which comprise our

zSecurity Pack, combine to offer a complete solution for  
your mobile assets, securing both hardware and data!

EX1026. A POSITA would have found it obvious to combine at least these two applications into a single application or program that satisfies a single “**security application**” construction. Combining these applications would have been obvious to try based on the above disclosures in zTrace and would have yielded predictable results as the combined single application would be capable of performing the same functions as the applications separately. EX1003, ¶¶94-96. These applications were already understood to co-exist in the hard drive together so it would have been a relatively elementary task for a programmer to combine them into a single application. *Id.*

Kesler provides further evidence that it would have been obvious to combine the applications into a single application. Kesler describes that its “tracing software includes a client part and a server part,” ([0023]), and “the client will reside in the computer’s hard drive,” ([0017]). In one embodiment, the client tracing software is described in terms of *modules* instead of applications, indicating that the software is comprised of a single “application” with multiple modules. Kesler, [0035] (“As shown in FIG. 3, the client tracing software 32 includes three main modules: zAgent 34, zCore 36, and zTrace 38. This architecture allows the zTrace software to use

system resources effectively and to be easily extended in the future.”), FIG. 3; EX1003, ¶¶97-98. Because Kesler’s sole inventor is also the creator of zTrace™, and Kesler teaches at least some zTrace™ functionality, it would have been obvious to try combining zTrace’s applications into a single application with multiple modules capable of performing specific functions, as described in Kesler. EX1003, ¶¶99-100.

For these reasons, zTrace discloses, suggests and/or renders this limitation obvious regardless of how PO interprets the claimed “**a security application.**”

**(d) Limitation 1[c][i]**

zTrace explains that owners must register their laptops with the zServer prior to receiving laptop protection. The main zTrace™ webpage provides a high-level overview of the zTrace™ services and includes a “Register now!” link that presumably leads laptop owners through a registration process. EX1004; EX1003, ¶¶101-102. On the FAQ webpage, the answer to question “How do I install zTrace?” is to “follow the registration and installation wizard on the zTrace web site[.]” EX1019, 2. The FAQ page also states that “[t]he information you entered during registration” is “used to notify you when your computer is found.” EX1019, 2.

zTrace also makes clear that the laptop itself is registered. For example, zTrace explains that when the owner purchases a new laptop, “[j]ust resubmit your

registration, and your new computer will be zTrace™ protected too.” EX1019, 3.  
“[Y]ou can simply cancel your subscription with [the old] computer.” *Id.* Thus,  
zTrace discloses that “**an owner of the mobile electronic device**” “**register[s] the  
mobile electronic device with a security service.**” EX1003, ¶103.

zTrace discloses that its “**security service resid[es] at least partially on one  
or more servers.**” zTrace discloses that the zTrace Gold application, once installed,  
communicates regularly with the zServer to check the status of the laptop (i.e.,  
whether or not it has been reported lost or stolen). EX1007 (“ZTRACE GOLD is...  
registered with the zServer with a unique identification. Every time the laptop is  
connected to the Internet, ZTRACE GOLD checks with the zSERVER to determine the  
laptop’s status.”). The zServer is part of the zTrace™ service.

A POSITA would have understood, or at least found it obvious, that at least  
the zTrace Gold application “**enabl[es]**” the owner to register her laptop with the  
zTrace™ service. EX1003, ¶105. zTrace explains that “zTRACE GOLD is installed on  
the laptop’s hard drive and registered with the zSERVER with a unique  
identification.” EX1007. This teaching indicates that the application is first installed  
and then registered with the zTrace™ service. EX1003, ¶105; *see also* Kesler, [0024]  
 (“As shown in FIGS. 1 and 2, the client part 12 is installed by the user on his  
computer 16. After registering 13, the user is automatically assigned a registration

number 15 that uniquely identifies the client in a database 20 associated with the tracing server 14.”). In other words, installing the applications onto the laptop ***enables*** the owner to register the laptop with zTrace™ services.

zTrace suggests that the installation and registration process is inextricably intertwined so you cannot have one without the other. For example, zTrace directs users to “the registration and installation wizard on the zTrace web site”—a single wizard to accomplish both tasks. EX1019, 2. A POSITA would therefore understand, or at least find it obvious, that by installing at least the zTrace Gold application onto the laptop, registration of the laptop is enabled because that application is registered with the zServer and now that application is associated with the laptop. EX1003, ¶106.

This is further evidenced by zTrace’s unsubscribe process. zTrace states that “you can unsubscribe from zTrace™ by uninstalling zTrace™ from your computer.” EX1019, 3. If the act of disassociating the zTrace software from the laptop is enough to “unsubscribe” from the zTrace™ service, then a POSITA would have understood, or at least found it obvious, that the opposite act of installing the software onto the laptop enables the zTrace™ service. EX1003, ¶107.

Thus, zTrace renders this limitation obvious.

**(e) Limitation 1[c][ii]**

This limitation is disclosed by the combination of zTrace and Kesler. EX1003, ¶¶108-120. zTrace suggests the functionality recited in this limitation and Kesler provides the details to render this limitation obvious.

zTrace explains how the zTrace Gold application functions:

zTRACE GOLD is installed on the laptop's hard drive and registered with the zSERVER with a unique identification. Every time the laptop is connected to the Internet, zTRACE GOLD checks with the zSERVER to determine the laptop's status.

EX1007. While zTrace is silent as to the relevance of the “unique identification” to the data communications and “determin[ing] the laptop's status,” Kesler explains that they are correlated.

Kesler discloses that “[a]fter registering 13, the user is automatically assigned a registration number 15 that uniquely identifies the client in a database 20 associated with the tracing server 14.” Kesler, [0024], FIG. 1 (at right). Kesler explains that this unique registration number, along with other identifying information (i.e., “the system ID of the computer,”

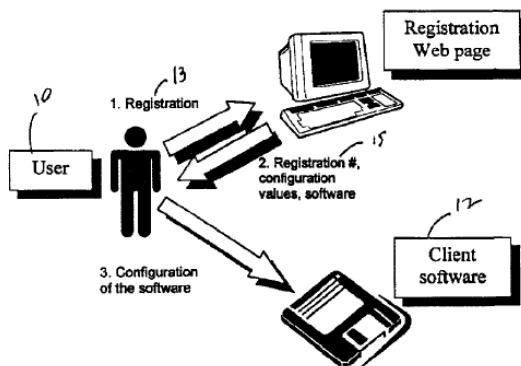


Figure 1

which is “unique by default”), is sent to the tracing server as part of a client report each time the client software connects to the Internet. Kesler, [0025], [0026], FIG. 2

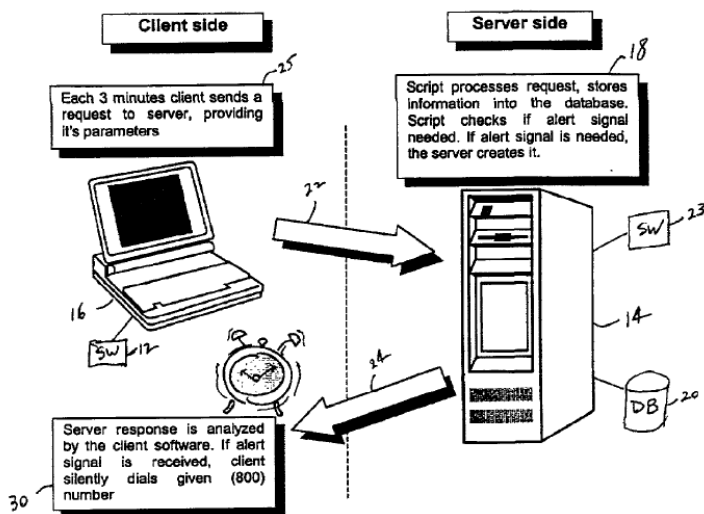


Figure 2

(at right, the client “provid[es] its parameters” to the server).

The server in Kesler uses this identifying information to determine whether it should respond to the client with an alert indicating the stolen status

of the laptop. Kesler [0027], [0034]-[0035], [0005].

It would have been obvious to a POSITA to combine Kesler with zTrace, predictably resulting in the zTrace Gold application sending the unique registration identification (and any other unique identifying information, such as a system ID) to the zServer each time the laptop connects to the Internet and checks in with the zServer to determine the laptop’s status. EX1003, ¶111. This combination would have been obvious to try with a reasonable expectation of success for at least the reasons discussed below as well as those previously discussed in connection with the intertwined disclosures of zTrace and Kesler. EX1003, ¶¶111-113. Modifying zTrace based on the disclosures in Kesler would have been easy and straight-forward

to implement as including this identifying information in zTrace Gold's check-ins with the zServer is a simple matter of sending data that the zTrace Gold application already possessed (i.e., the assigned registration number) to the zServer. *Id.* zTrace also had access to "[s]ystem serial numbers" for the laptop via the zAsset Track application and could have easily acquired and sent that information to the zServer as well. *Id.*; EX1016.

The disclosures in Kesler also provide teachings, suggestions, and motivations for this combination and resulting functionality. EX1003, ¶¶114-115. Kesler explicitly identifies a "zTrace" module, (Kesler, [0035]), that "controls... gathering of the identifying information and tracing of the computer's location" consistent with the above disclosures, (*id.*, [0037]). As Dr. Polish explains, the "zTrace" module in Kesler functions similarly to the zTrace Gold application and a POSITA would have been motivated to modify the zTrace Gold application so that it gathers and sends identifying information to the zServer as part of its communications, similar to the "zTrace" module in Kesler. EX1003, ¶115.

It was well known by August 2003 to send identifying information to the devices on the receiving end of a data communication, as this was one of only a few ways for a transmitting device to identify itself to a receiving device. EX1003, ¶116; Isikoff, 9:53-63 (a laptop "transmitting its ID"), 9:64-10:10, 10:11-31; Cotichini,

3:54-4:7 (“signals contain the encoded identification (serial number) of the sending computer”), 4:15-29, 8:33-51, 16:1-9; 30:34-37. In the case of zTrace, some identifying information would be needed for the zServer to “determine the laptop’s status,” which is the purpose of the zTrace Gold application communicating with the zServer. EX1007; EX1003, ¶117. Without such identifying information, the main purpose for the zTrace Gold application would be thwarted because the zServer would be unable to alert the application that the laptop has been stolen and instruct the application to provide its location so that the recovery process can begin. *See* EX1007; EX1006; EX1003, ¶117. This would render zTrace™ services useless.

For these reasons, it would have been obvious for zTrace Gold to “**caus[e] the mobile electronic device [i.e., laptop] to automatically send [i.e., at every Internet connection] identifying information for the mobile electronic device [i.e., the unique registration identification and/or other identifying information such as a system ID] to the security service [i.e., via the zServer],**” based on the disclosures of Kesler. EX1003, ¶¶118-120; *see also* limitation 1[c][iii].

**(f) Limitation 1[c][iii]**

This limitation is rendered obvious by the combination of zTrace and Kesler. EX1003, ¶¶121-131. As previously discussed, as part of the registration process, zTrace Gold is installed on the subscriber’s laptop and protection via the security

service begins. *See* limitation 1[c][i] above; EX1007. Then, “[e]very time the laptop is connected to the Internet, zTRACE GOLD checks with the zSERVER to determine the laptop’s status.” EX1007. Therefore, **“after the owner has registered the mobile electronic device with the security service,”** zTrace Gold **“caus[es] the mobile electronic device to... communicate with the security service.”** Because it is known that no Internet connection and communication is possible when the laptop is turned off, zTrace also suggests or renders obvious that such communication occurs **“when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off.”** EX1003, ¶¶122-123.

Kesler also teaches **“periodically communicat[ing]”** with a remote server. Kesler discloses that its client tracing software checks for an Internet connection every 20 minutes and then communicates with the server if an Internet connection is detected. Kesler, [0032] (“[e]very N2 (for example, 20) minutes (according to the system timer 2) the client tracing software checks for an Internet connection 46, and checks the availability of the server 48 and (if available) sends all data available at that moment in the data stack to the server.”).

It would have been obvious to combine Kesler’s periodic communication approach with zTrace, predictably resulting in the zTrace Gold application

communicating with the zServer every time the laptop connected to the Internet *and* at pre-determined intervals. EX1003, ¶¶124-126. Periodic communication was well known in the art by August 2003 so a POSITA would have known how to implement this trivial feature into zTrace and would have had every reasonable expectation of success. *See, e.g.*, Cotichini, 3:1-17, 11:32-50, 20:60-67, 30:7-11; Isikoff, 9:64-10:10; EX1003, ¶126. This modification would have been obvious to try for the same reasons as well as those discussed throughout in connection with the overlapping disclosures of zTrace and Kesler.

A POSITA would have realized the benefits of having zTrace periodically communicate with the security service using both approaches. EX1003, ¶¶127-130. Kesler explains that connecting at regular intervals “reduces the need to synchronize the local and server timelines.” Kesler, [0033]; EX1003, ¶129. Connecting at periodic intervals also allows the zTrace Gold application to more frequently check for any changes in the laptop’s status and location. EX1024; EX1028; EX1020; EX1003, ¶¶127-128 (opining on benefits realized from continuing to check in with the zServer at intervals even after the laptop has been reported stolen).

**(g) Limitation 1[c][iv]**

This limitation is rendered obvious by (1) zTrace alone, (2) by zTrace in view of Kesler, or (3) by zTrace in view of Isikoff and/or Kesler. EX1003, ¶¶132-152.

As discussed for limitation 1[c][i], as part of the registration process, zTrace Gold is installed on the subscriber's laptop and then protection via the security service begins. The following functionality in zTrace occurs **“after the owner has registered the mobile electronic device with the security service.”**

zTrace discloses that “[i]n the event of theft, the owner notifies the zTrace Monitoring Center via phone, e-mail, fax, or the Web” and the “zServer tracking system is activated and waits for the next connection of that laptop to the Internet.” EX1022; EX1019, 3 (instructions to the laptop owner for reporting theft); EX1028. The brochure describing zTrace Gold's functionality explains the application's next steps: “[w]hen the missing computer connects to the Internet, the stealth application receives a signal from the zServer and the computer reports its own location.” EX1007; *see also* EX1028. The zTrace Gold application therefore **“accept[s] [i.e., receives] a notification [i.e., the signal] at the mobile electronic device [i.e., the laptop] from the security service [i.e., the zServer].”**

This signal is understood to be **“a message”** to the zTrace Gold application **“indicating that the owner of the mobile electronic device has reported a loss,”** as this signal is sent as a direct result of the laptop being reported missing and triggers the application to perform a task (i.e., “report[] its own location”) that is invoked when the laptop is reported missing. *See* EX1007 (“*If the laptop is reported*

*missing*, a patent pending process occurs for the zTrace Recovery Team to identify the computer's exact physical location;" zTrace Gold "pinpoint[s] [the] actual location of the *missing* laptop"); EX1006; EX1028; EX1003, ¶135.

Kesler confirms the details about the zServer's messaging. Kesler discloses that its "tracing server will communicate with the stolen computer, notifying it that it was stolen." Kesler, [0017]; *see also id.*, claim 10. It would have been obvious to modify zTrace, based on the disclosures of Kesler, so that the zTrace Gold application receives a message from the zServer notifying it that the laptop has been reported stolen. EX1003, ¶¶136-137. Combining zTrace with Kesler in this manner would have been obvious to try. *Id.*, ¶¶137-138. As discussed throughout, Kesler's sole inventor created the zTrace™ service and Kesler includes embodiments that explicitly identify "zTrace" modules. A POSITA would have been motivated to look to Kesler's teachings for more details about the signal received at the zTrace Gold application from the zServer and would have found it obvious to try implementing Kesler's notification/message in zTrace. *Id.*

The combination results in a trivial modification that would have been straight-forward to implement with a reasonable expectation of success, as the only real change to zTrace (if any at all) is with the content of the signal/message sent from the zServer to the zTrace Gold application. EX1003, ¶139. zTrace explains that

the zTrace Gold application is designed “to determine the laptop’s status” and then “trace[] the location of missing laptops for recovery”—a message notifying the application that the laptop is stolen would further the application’s purpose. *Id.* A POSITA would have been further motivated to combine Kesler with zTrace for the reasons discussed in previous limitations 1[c]-1[c][iii].

For the reasons set forth above, zTrace alone or zTrace in combination with Kesler renders obvious “**accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss.**”

Limitation 1[c][iv] recites in the alternative that “**the notification comprises a message indicating that the owner of the mobile electronic device has... requested disabling of the mobile electronic device.**” This element is rendered obvious by zTrace alone or by zTrace in view of Isikoff.

With respect to zTrace alone, as previously discussed, the zControl application “provides automated control of the computer’s data.” EX1013. Through the zControl web-based interface, an owner of the missing computer can communicate with his/her computer and “render the whole computer useless by locking its keyboard and mouse.” EX1053; *see also* EX1026; EX1028; EX1013. A POSITA would have understood, or at least found it obvious, that the zControl

application receives these directives to disable the laptop from the zServer in the form of a “**message**,” as the zServer is the only component of the zTrace™ service provider that communicates with the laptop and the zControl application must receive (or “**accept[]**”) these directives to execute them. EX1003, ¶¶142-143 (also opining that this configuration would have been obvious to try because of the limited number of ways the zTrace™ service provider can communicate with the applications within the laptop). For these reasons, zTrace alone renders obvious **“accept[ing]... a message indicating that the owner of the mobile electronic device has... requested disabling of the mobile electronic device.”**

To the extent additional details are required to satisfy this claim element, they are disclosed by Isikoff. Isikoff discloses a mobile device with a beacon capable of receiving device control signals from a remote user, including signals to disable the mobile device, after the mobile device has been reported stolen. Isikoff, Abstract (“wherein a beacon or transceiver in the computer implements file integrity or device recovery steps.... When activated as a security device, [the beacon] implements strategic machine control including enabling, disabling, or modifying functions of the computer and communication of data.”), 3:46-50, 4:3-14. Isikoff explains that, when the laptop is reported stolen, the beacon receives “low-level control codes” that instruct the beacon to “implement at least some of the security features of the

device... includ[ing] the disabling or interruption of power to all or to specific parts of the computer,... or to the erasure of the hard drive.” Isikoff, 5:59-6:5; *see id.*, 6:17-30. The disabling and other security measures “may be set in advance” or “may be controlled by an external communication, in which case the user... may make the decision as to which of these steps is appropriate.” Isikoff, 3:46-54. In other words, a remote user is controlling which security functions the beacon executes. EX1003, ¶144.

It would have been obvious to modify zTrace based on the general teachings of Isikoff because it would have predictably resulted in the zControl application receiving a message (e.g., in the form of a code) from the zServer with instructions from the owner to disable the laptop. EX1003, ¶145. The remote user at the zControl web-based interface can send directions to disable the laptop to the zServer, which then forwards the directions to the zControl application for execution. *Id.* Or, the disable message could be pre-set by the owner (e.g., as part of the registration process) so that the message is automatically sent from the zServer to the zControl application as soon as the laptop is reported stolen, as similarly described in Isikoff. Isikoff, 3:46-54; EX1003, ¶145; *see also* limitation 1[c][v] discussions related to this pre-set disable messaging.

zTrace explicitly discloses the use of “[p]redefined actions,” which include

“retrieving files, [and] deleting sensitive information,” and explains these “[a]ctions can be triggered by... a zTrace loss report.” EX1013. It would have been obvious to include the disable feature as a predefined action because it would have furthered zControl’s objective, which is to “provide[] automated control of a computer’s data even AFTER loss has occurred,” as well as the overall zTrace™ service’s objective, which is to “protect[] sensitive data in case of unauthorized access[.]” EX1013; EX1005; EX1003, ¶146 (explaining that this modification would have been trivial).

zTrace teaches the use of disabling functionality. A POSITA would have therefore been motivated to seek more information about how to implement this functionality and would have considered Isikoff because of its details on remotely disabling mobile devices that have been reported lost or stolen. Isikoff, 1:59-65; EX1003, ¶147. The concept of remotely disabling devices was well known in the art by August 2003. EX1003, ¶148; EX1037, 214. For these reasons and those identified above, it would have been obvious to try combining zTrace with Isikoff. EX1003, ¶149. Additionally, any modifications to zTrace because of this combination would have been straight-forward to implement and there would be a reasonable expectation of success. EX1003, ¶¶146, 149.

Furthermore, to the extent the claimed “**security application**” is considered a single application as discussed for limitation 1[c], a POSITA would have understood

that the single application formed by the zTrace Gold and zControl applications would have performed the above functionality. For example, it would be the single application that receives both types of messaging from the zServer. EX1003, ¶150.

Isikoff is analogous art to zTrace and Kesler, as it teaches a similar mobile device protection and tracking system. Isikoff, 1:59-65; EX1005; Kesler, [0015]-[0017]. Both Isikoff and Kesler teach functionality that is already explained in zTrace at a high level. It therefore would have been obvious to further combine Isikoff with Kesler to the extent needed to render obvious limitation 1[c][vi], as the relied-on functions of Isikoff and Kesler are independent of each other and can be implemented separately to enhance the functionality of zTrace. EX1003, ¶151.

**(h) Limitation 1[c][v]**

As just discussed, zTrace alone or zTrace in view of Kesler renders obvious that the zTrace Gold application receives a “**notification**” indicating that the laptop has been reported stolen, and zTrace alone or zTrace in view of Isikoff renders obvious that the zControl application receives a “**notification**” indicating that the owner has requested that the laptop be disabled. EX1007; EX1022; EX1019, 3; EX1013; EX1026; EX1053; EX1028; *see* limitation 1[c][iv] above. The claimed “**automatically disabling**” can occur “**in response to receiving**” either one of these “**notification[s]**.”

With respect to the notification being a disable request, zTrace explains that the zControl application allows owners to “render the whole computer useless by locking its keyboard and mouse,” which would disable “**at least one user function of the mobile electronic device**”—i.e., keyboard or mouse inputs. EX1053; *see also* EX1028; EX1026. zTrace touts that the zControl application “provides automated control of a computer’s data.” EX1013. A POSITA would have understood that this disabling occurs “**automatically**” as all actions taken by the zControl application on the laptop are without user input at the laptop. *See* EX1026 (“zControl is stealth software that provides automated, remote and invisible control”); EX1028; EX1053; EX1003, ¶¶153-156; *see also* Isikoff, 3:46-53, 4:3-14.

Additionally, as previously discussed, zTrace discloses the use of predefined actions that the zControl application executes in response to receiving a “**notification**” that the laptop is reported stolen or a request to disable the laptop. EX1013. The predefined actions can be stored at the laptop and executed by the zControl application after the zTrace Gold application receives a notification from the zServer that the laptop is reported stolen. EX1003, ¶157; Kesler, FIG. 1. As previously discussed in connection with limitation 1[c], these applications work together cooperatively to provide the zTrace™ service.

A POSITA would also recognize the obviousness of an alternative

configuration: the predefined actions can be sent from the zServer to the zControl application as discussed for limitation 1[c][iv] and in view of Isikoff, and then zControl executes that action upon receiving the notification from the zServer. It would have been obvious to include the disable feature as a predefined action in zTrace, as such features were known in the art by August 2003, as evidenced and rendered obvious by Isikoff for limitation 1[c][iv]. EX1003, ¶¶158-159; Isikoff, 3:46-54 (explaining that disabling features “may be set in advance”).

As also discussed for limitation 1[c][iv], including the disable feature as a predefined action would have furthered the objectives of both zControl and the zTrace™ service, which are to “provide[] automated control of a computer’s data even AFTER loss has occurred” and “protect[] sensitive data in case of unauthorized access,” respectively. EX1013; EX1005; EX1003, ¶¶159-60. In this instance, the zControl application would “**automatically disabl[e] at least one user function of the mobile electronic device**” based on the predefined actions and in response to the “**notification**” that the laptop is reported stolen or a request to disable the laptop.

As also discussed for limitation 1[c][iv], to the extent the claimed “**security application**” is considered a single application, a POSITA would have understood that the single application formed by the zTrace Gold and zControl applications would have performed the above functionality. EX1003, ¶161.

Limitation 1[c][v] further requires that the “**disabling**” occurs “**while still allowing the mobile electronic device to communicate with the security service.**”

As discussed for limitation 1[c], the zControl and zTrace Gold applications cooperatively work together to protect data on a laptop in the event it is stolen. *See* EX1052 (identifying a “zSecurity Pack”); EX1026. zTrace explains that “[t]he computer completes a handshake with the zServer at *every* Internet connection.” EX1007; EX1006. This indicates that the zTrace Gold application is functional at the same time as the zControl application. EX1003, ¶162.

It would have been obvious to maintain communication with the zServer after one or more functions of the laptop have been disabled for at least the same reasons discussed for limitation 1[c][iii] related to continuing periodic communication with the zServer after the device is reported stolen. EX1003, ¶163. Here, continuing communication with the zServer after one of more user functions have been disabled would allow the laptop’s location to be tracked if it was moved to a new location and would allow the owner to maintain control of the laptop while it remains missing, by enabling later-provided instructions for copying, retrieving and then deleting data from the laptop to be received and executed. *See* EX1013 (“zControl... enables personal control of the computer’s data even AFTER theft or loss”); EX1003, ¶¶163-165; EX1053; EX1026. This would advance zTrace™ service’s

objective to “protect[] sensitive data in case of unauthorized access[.]” EX1005; EX1003, ¶¶163-165.

For at least these reasons, this limitation is rendered obvious by zTrace alone, zTrace in view of Kesler and/or zTrace in view of Isikoff.

**(i) Limitation 1[c][vi]**

zTrace discloses this limitation. The zControl application in zTrace executes predefined actions, including “retrieving files,” in response to a laptop being reported stolen. EX1013 (“Action can be triggered by... a zTrace loss report. Predefined actions can include retrieving files...”); EX1012 (“zControl... retrieves files”). These files, which are the property of the laptop owner, are the claimed **“at least some user data.”** Files that are retrieved from the laptop are understood to be **“copied from the mobile electronic device,”** as will be discussed further below. EX1003, ¶167. And because the zControl application performs these predefined actions in response to the laptop being reported stolen, without user input at the laptop, they are **“automatic[].”** The zControl application is therefore understood to **“automatically caus[e] at least some user data to be copied from the mobile electronic device.”** See limitation 1[c][v] above (discussing how zControl is “automated”); EX1013; EX1026; EX1053; EX1028; EX1003, ¶¶167-175.

In the context of real-time instructions sent from a remote laptop owner to the

zControl application, zTrace explains that the owner can “recover the files from the stolen computer by uploading them to the zTrace server.” EX1053; *see also* EX1026. It is obvious that “recover” here refers to the data being “**copied from the mobile electronic device to at least one of the servers.**” EX1003, ¶¶168-170. A POSITA would have understood, or at least found it obvious, that this copying functionality also applies to any files or data retrieved or recovered as a result of any predefined actions, as this would have allowed the owner to regain possession of those files/data. EX1003, ¶¶168-175; *see also* Isikoff, 8:22-61 (disclosing similar copying functionality performed by predefined actions).

**(j) Limitation 1[d]**

This limitation is disclosed by zTrace or, alternatively, is rendered obvious by zTrace in view of Bonnett.

As discussed for limitation 1[b], the laptop in zTrace includes a hard drive. EX1019, 2. A hard drive is a “**non-volatile memory.**” EX1001, 22:13-18 (“a ‘nonvolatile’ memory device... means that the memory contents remain intact even when the computer [] powers down”); EX1036, 56 (PO’s infringement contentions identifying a “hard drive” as a “memory”); EX1003, ¶¶176-177 (citing EX1037, 433, 481). Thus, zTrace alone discloses this limitation.

To the extent PO argues a construction for “**non-volatile memory**” that

excludes a hard drive, then this limitation is generally disclosed by Bonnett. Bonnett describes methods for securing software within a computing device memory to prevent a user from intentionally or accidentally altering or corrupting the program. *See* Bonnett, [0006]-[0007], [0011], [0019], [0024]. The device in Bonnett includes a memory 124 that may be “a NAND flash memory, or any other suitable volatile or nonvolatile storage and retrieval device or combination of devices.” Bonnett, [0031]; *compare to* EX1001, 19:8-13 (describing a “Flash memory 4500 containing a changeable area 4510 and a system area 4520”), FIG. 45 (illustrating “Flash memory 4500”).

It would have been obvious to a POSITA to modify the laptop in zTrace to include another type of memory component, such as a flash memory or “nonvolatile storage and retrieval device,” in addition to the hard drive. EX1003, ¶¶178-183. It was common for computing devices by August 2003 to include multiple memory components—even zTrace discloses two memories (e.g., a “16 MB RAM, [and a] HD”). EX1019, 2; EX1003, ¶180. Adding an extra memory component would allow the laptop to store more programs and provide enhanced functionality to the owner. EX1003, ¶181. Adding another memory component to the laptop would have been easy as most laptops were equipped with extra space for additional cards and components. *Id.* Thus, this modification could be accomplished without undue

experimentation and with a reasonable expectation of success, without any change in functionality to the hard drive or other components. *Id.*

A POSITA would have looked to Bonnett for non-volatile memory related disclosures because both zTrace and Bonnett are in the computing arts and involve concealing software from device users. Bonnett, [0011]; EX1019, 2; EX1007; EX1013. Both references also disclose the use of non-volatile memories to hide their software (as will be discussed more in the next sections)—Bonnett is merely relied on to describe a non-hard-drive-type of non-volatile memory in the event PO provides a narrow construction that excludes a hard drive as a non-volatile memory. EX1003, ¶186.

Including an additional memory component into zTrace’s laptop would have also been an obvious design choice because, as Dr. Polish explains in his declaration, the components in the laptop were well known off-the-shelf components that could be used interchangeably. EX1003, ¶¶184-185; *see* Forbes, 1:35-44; *see also* limitations 1[a] and 1[b]. A POSITA would have known that a flash memory is one of only a few types of non-volatile memory that could operate in conjunction with a processor in a computer so it would have been obvious to try modifying zTrace’s laptop to include a flash memory or other “nonvolatile storage and retrieval device,” as disclosed in Bonnett. EX1003, ¶¶182-183. As will be discussed in more detail for

limitation 1[f], the flash memory would have further been capable of storing the zTrace applications. Flash memory, in particular, was very popular by August 2003, especially for use in mobile devices, such as laptops. *See* Bez, 489, 491; Goronkin, 806; EX1003, ¶185.

Additional motivations to combine these two references discussed in connection with limitations 1[e] and 1[f] also apply here.

With respect to Kesler and Isikoff, these references are also in the computer arts and involve concealing software from unauthorized device users and are therefore complementary references to Bonnett. Kesler, [0015]; Isikoff, 1:59-65. Kesler describes embodiments of zTrace™ so a POSITA would be motivated to combine Kesler with Bonnett for the same reasons discussed for zTrace. EX1003, ¶187. Isikoff is relied on for the limited purpose of teaching disabling laptop features, which would not be impacted by including additional memory in the zTrace laptop. *Id.*

For these reasons, limitation 1[d] is also rendered obvious by zTrace in view of Bonnett.

**(k) Limitation 1[e]**

Regardless of how PO interprets “**non-volatile memory**,” this limitation is rendered obvious based on the combined disclosures of zTrace and Bonnett.

**FIG. 2**

FIG. 2 is a block diagram of a system 200. The system 200 is enclosed in a dashed rectangular boundary. Inside the boundary, there is a cylinder 206. The cylinder 206 is divided into two sections: a blue section 206a and a light blue section 206b. Section 206a contains a purple rectangle 225a and a white rectangle 216. Section 206b contains a purple rectangle 225b and a white rectangle 220. A dashed line 208 points from section 206a to a block 214. A dashed line 210 points from section 206b to a block 202. Above the dashed box, there is a block 213 connected to a line 205, which points down to block 204. Block 204 points down to block 214. Block 202 points up to block 214. The entire dashed box is labeled 200 on the right.

-51-

software... and/or any other desired information” “that a program designer desires to be made inaccessible to a user” of the device (represented as 225b in purple above). Bonnett, [0036]; *see also id.*, [0037], claim 1.

A POSITA would have understood that the open partition described in Bonnett acts as a “**changeable area that can be modified by a user**,” as that partition is “accessible to the user.” EX1003, ¶¶190-195. A POSITA would also have understood that the hidden partition described in Bonnett acts as a “**system area that cannot be modified by the user**,” because that partition is “made inaccessible to [the] user.”<sup>4</sup> *Id.*

If the claimed “**non-volatile memory**” includes a hard drive, then it would have been obvious to combine zTrace with the general disclosures of Bonnett so that

---

<sup>4</sup> This interpretation of the “**changeable area**” and the “**system area**” is consistent with PO’s application of these claim terms in its infringement contentions in the parallel district court litigation. For example, for this limitation, PO stated that systems “either provide access to certain files (e.g., files stored in a changeable area) or restrict access to certain files (e.g., files stored in a system area that cannot be modified by a user).” EX1036, 59. It concluded that “[t]he Application agent is not changeable by a user and therefore resides at least partially in the system area.” *Id.*

the hard drive in zTrace includes an open partition that is accessible to the laptop user and a hidden partition that is not accessible to the laptop user. EX1003, ¶196. In this manner, the hard drive in zTrace would include the claimed “**changeable area**” and “**system area**.”

zTrace already suggests the zTrace Gold application is stored in a hidden or otherwise secure area on the hard drive. For example, zTrace discloses that “zTRACE GOLD is undetectable and unerasable on [the] laptop’s hard drive.” EX1007. Dr. Polish explains that an application that is “undetectable” on a hard drive is understood to be hidden on the hard drive. EX1003, ¶197. And, when that application is “unerasable” on the hard drive, it means that the application cannot be changed, as erasing is the ultimate form of change. *Id.* To achieve these characteristics, Dr. Polish opines that the hard drive in zTrace is understood to include a hidden or otherwise secure area in which the zTrace Gold is stored. *Id.* (citing to EX1019, 2-3; Kesler, [0017] (the client software is “installed onto track zero” of the hard drive, which is known to be a hidden track on the hard drive)).

zTrace also suggests that the zControl application is stored in a hidden area. For example, zControl is described as an “invisible software application.” EX1013; EX1026; EX1003, ¶¶198-200. An application that is invisible is undetectable and thus, for the same reasons just discussed, a POSITA would have understood that the

zControl application is also stored in a hidden or otherwise secure area. *Id.*

zTrace therefore provides teachings, suggestions and motivations to combine with Bonnett. EX1003, ¶¶197-200. Bonnett further provides teachings, suggestions and motivations to combine with zTrace because it discloses that the hidden partition and open partition can be implemented in a “nonvolatile storage and retrieval device” and a hard drive is a well-known “nonvolatile storage and retrieval device.” Bonnett, [0031]; EX1003, ¶201. Thus a POSITA would have been motivated to look to Bonnett for details on how the hard drive in zTrace’s laptop was configured and where on the hard drive the zTrace Gold and zControl applications should be located so they remain hidden from the user. EX1003, ¶201.

It also would have been obvious to try combining Bonnett with zTrace for the same reasons. EX1003, ¶¶202-203. It would have been obvious to look to Bonnett for more explicit disclosures of the hidden area (“**system area**”) already suggested in zTrace. *Id.* With respect to a “**changeable area**,” it was well known that hard drives include areas that users can access and modify so a POSITA would have understood that zTrace’s hard drive would also include such an open area. *Id.* Furthermore, as discussed for limitation 1[d], modifying zTrace’s laptop to include an additional memory component would have been an obvious design choice, as the laptop itself consists of off-the-shelf components that have known features and

benefits. EX1003, ¶204.

Consistent with the disclosures in zTrace, and the complementary disclosures in Kesler describing similar functionality, Bonnett explains that storing programs within a hidden memory partition is “advantageous” because it “substantially prevent[s] a user from deleting and/or corrupting those... program[s].” Bonnett, [0037]. This results in an “improved reliability” of the program and the device executing the program. *Id.* Such disclosures reinforce the need for zTrace’s applications to remain “invisible” on the hard drive and provide further motivation for the applications to be located in a hidden portion of the hard drive. EX1003, ¶205.

For these reasons, zTrace in view of Bonnett render obvious that **“the non-volatile memory [i.e., the hard drive] comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user.”**

If the claimed “**non-volatile memory**” excludes a hard drive, then the laptop in zTrace is modified to include another type of memory component, such as a flash memory or other “nonvolatile storage,” in addition to the hard drive, as discussed for limitation 1[d]. Bonnett explicitly discloses that such flash memory and other nonvolatile storage can include an open partition and a hidden partition. Bonnett, [0031]-[0033]. It therefore would have been obvious for the additional memory

component within the modified zTrace laptop to include a hidden partition and an open partition. Bonnett, [0007], [0031]-[0037]; EX1003, ¶¶207-208.

Additional reasons and motivations for combining Bonnett with zTrace to disclose a “**changeable area**” and a “**system area**” will be made apparent in the next section.

### (I) Limitation 1[f]

The combined disclosures of zTrace and Bonnett render this limitation obvious. EX1003, ¶¶209-218.

In instances where the “**non-volatile memory**” includes a hard drive, it would have been obvious to a POSITA to combine zTrace and Bonnet based on the discussion above for limitation 1[e] so that the zTrace Gold and zControl applications (collectively, “**the security application**”) are in a hidden partition (i.e., “**system area**”) of the laptop’s hard drive that is “inaccessible to the user,” as described in Bonnett. *See supra*; Bonnett, [0007], [0031]-[0037]; EX1003, ¶210. This configuration is consistent with the teachings of zTrace, which suggest the use of a hidden area on the hard drive to keep the applications “invisible” or “undetectable” to the laptop user. *See* EX1007; EX1013; EX1026; EX1053; EX1019, 2-3; *see also* Kesler, [0017] (track zero); EX1003, ¶210. A POSITA would have understood that the processor-executed “applications” in zTrace refer to

“code.” EX1003, ¶211. Thus, if the claimed “**non-volatile memory**” includes a hard drive, then zTrace in view of Bonnett discloses or renders obvious “**wherein the security application utilizes codes residing at least partially in the system area.**”

*Id.*

If the claimed “**non-volatile memory**” excludes a hard drive, then it would have been obvious to combine zTrace with Bonnett so that the zTrace Gold and zControl applications are stored within a hidden partition of the additional memory component, e.g., a flash memory or other non-volatile storage and retrieval device, as opposed to the hard drive, so that the applications remain “invisible” or “undetectable” to the laptop user. EX1003, ¶¶212, 216. A POSITA would have understood that the processor executes applications the same way regardless of where the applications are stored in the laptop. *Id.* In this manner, the additional memory component would be responsive to the processor in zTrace in the same way as the hard drive. *See* limitation 1[b] above; EX1003, ¶212. This combination could therefore be achieved with a reasonable expectation of success.

The reasons to combine Bonnett with zTrace discussed for limitations 1[d] and 1[e] apply here. For example, it would have been obvious to try including an additional memory component, such as a flash memory, and installing the zTrace Gold and zControl applications within the hidden area of the additional memory

component, as this would have allowed the applications to remain hidden to the user of the laptop. EX1003, ¶¶213, 216. The additional memory component would respond to the processor and execute the applications the same way as it would if they were on the hard drive so that modification could be achieved with a reasonable expectation of success and without any change to the functionality of the applications. *Id.*

Furthermore, installing the zTrace™ applications in a memory component outside of the hard drive may provide an added layer of protection for the laptop. Stolen computers are often stripped for their parts and hard drives are commonly removed in the process. *See* Cotichini, 21:22-32. If the zTrace applications reside on the hard disk and the hard disk is removed from the laptop, then the zTrace applications are rendered useless and the zTrace™ service fails. EX1003, ¶214. With this understanding, a POSITA would have recognized the benefit of moving the zTrace applications off the hard drive and onto another memory to avoid this common pitfall and to ensure that the zTrace™ service remains active even if the hard drive is removed from the laptop. EX1003, ¶¶214-215.

The reasons to combine Bonnett with Kesler and Isikoff described above for limitation 1[d] apply here. They are analogous references concerned with concealing software from unauthorized laptop users so a POSITA would have been motivated

to look to these references for details about how to implement certain features of the applications and the hardware on which they reside so that the applications remain hidden from the unauthorized users. *See* Kesler, [0015]; Isikoff, 1:59-65; Bonnett, [0007], [0011], [0019]. Bonnett recognizes that keeping these software applications hidden “prevent[s] a user from deleting or corrupting” the program, which “improve[s] reliability” of the laptop. Bonnett, [0011]. The application features added by Kesler and Isikoff are not affected by the addition of a memory component. EX1003, ¶¶215-217.

For these reasons, this limitation obvious is rendered obvious by zTrace in view of Bonnett.

**(m) Limitation 1[g]**

This limitation is also rendered obvious by zTrace in view of Bonnett. The claimed “**notification**” here first appears in limitation 1[c][iv]. For that limitation, Petitioners demonstrated that the zTrace Gold application receives messages from the zServer indicating that the laptop has been reported stolen (as disclosed by either zTrace alone or in combination with Kesler). *See, e.g.*, EX1007; EX1022; Kesler, [0017], claim 10. Petitioners further demonstrated that the zControl application receives messages from the zServer indicating that the owner of the laptop has requested disabling of the laptop (as disclosed by either zTrace alone or in

combination with Isikoff). *See, e.g.*, EX1013; EX1026; EX1053; EX1028; Isikoff, Abstract, 3:46-53, 4:3-14, 5:59-6:5, 6:17-30. Thus, for the reasons discussed for limitation 1[c][iv], zTrace, either alone or in combination with Kesler and/or Isikoff, discloses that “**the security application receives the notification from at least one of the servers.**” EX1003, ¶219.

Limitation 1[g] adds that the notification is received “**via the system area.**” This language does not appear in the ’649 patent. At best, the ’649 patent describes an embodiment where a flash memory 4800 system area 4820 includes an application component 4840 that “communicates with web servers 4870a, 4870b,... 4870n... through an Internet connection 4845.” EX1001, 20:8-31, FIG. 48; *see also id.*, 19:8-26, FIG. 45, 33:24-34:46 (discussing the different types of messages received by an “application component located in the system area”). Based on this limited disclosure, it appears that this claim element is satisfied merely by storing within a system area 4820 an application component 4840 capable of communicating with a server 4870a-n. This is consistent with how PO applied this claim element in its infringement contentions in the parallel district court litigation. It concluded that “[t]he entire [security] application agent [] resides in a system area and therefore the security application receives the notification from at least one of the servers via the system area.” EX1036, 72.

When zTrace is modified by Bonnett as discussed for limitations 1[d] to 1[f], the zTrace Gold and zControl applications reside in a hidden partition of the laptop's hard drive or other secondary memory and receive the notification from the zServer. Thus, consistent with the PO's interpretation of this claim limitation, a POSITA would have understood that the applications receive the notification “**via the system area.**” EX1003, ¶¶220-221. Alternatively, in light of zTrace's and Bonnett's teaching, a POSITA would have known it was an obvious design choice for the security application to receive notifications from a security server “**via the system area**” because it would promote zTrace's and Bonnett's express teachings to prevent thieves from thwarting the operation of the security system by concealing the application and preventing its modification or removal, which would extend to functionality for communicating with a security server. *See* Bonnett, [0011], [0037]; EX1007; EX1013; EX1026; EX1053; EX1019, 2-3; Kesler, [0009], [0017]; EX1003, ¶222.

The reasons for combining the prior art – zTrace, Bonnett, Kesler and/or Isikoff – are the same as discussed for limitations 1[d] through 1[f]. EX1003, ¶¶223-224.

For these reasons, claim 1 is rendered obvious by zTrace in view of Kesler, Isikoff and/ Bonnett.

## 2. Independent claim 9

Claim 9 recites a method claim with limitations that are substantively identical to those in claim 1. The arguments presented above for claim 1 therefore apply to claim 9. A complete side-by-side comparison of claim 9 to claim 1 is provided in Dr. Polish's declaration. EX1003, ¶226. Only limitations with notable differences are shown side-by-side below and discussed separately. (Additions are underlined and deletions are in strikethrough.)

As a preliminary matter, method claim 9 is broader than device claim 1 because at least limitations 1[c][i] to 1[c][vi] are required to be performed by a **“security application,”** whereas claim 9 is not so specific. Also, method claim 9 does not recite **“a processor”** or **“one or more non-transitory machine-readable storage media responsive to the processor.”** EX1003, ¶¶227-228.

| Notable claim 9 limitations                                                                                                                                                                                                        | Notable claim 1 limitations                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9[pre]. <u>A method for providing security for</u> a mobile electronic device, <u>the method</u> comprising:                                                                                                                       | 1[pre]. A mobile electronic device, comprising:                                                                                                                                           |
| 9[a] <u>receiving, at a mobile electronic device, a request from</u> an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers; | 1[c][i] <del>enabling</del> an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers; |
| 9[b] <u>in response to the request from that owner, registering the mobile electronic device with the security service;</u>                                                                                                        |                                                                                                                                                                                           |

**(a) Preamble**

zTrace discloses implementing security software in “laptop computers,” which are “**mobile electronic device[s]**.” EX1019, 2; EX1006; EX1003, ¶229. The software is part of the overall zTrace™ service that “aids in the recovery of stolen or missing computers, protects sensitive data in case of unauthorized access and effectively monitors hardware and software assets for tracking.” EX1005. Thus, zTrace discloses “[a] **method for providing security for [the] mobile electronic device.**”

**(b) Limitation 9[a]**

Limitation 9[a] adds “**receiving, at a mobile electronic device, a request from [the] owner... to register.**” The remaining portion of this limitation is identical to limitation 1[c][i], the relevant arguments for which apply here. It is obvious that the owner would use her laptop to complete the registration for the zTrace™ service. *See, e.g.*, Kesler, FIG. 1. For example, the owner would have used her laptop to navigate to the main page of the zTrace.com website [EX1004], shown in excerpt and annotated below, which includes a “Register now!” link.



A POSITA would have understood that clicking the “Register Now!” link would have resulted in the laptop “receiving... a request from [the] owner... to register” the laptop. EX1003, ¶231. A POSITA would have further understood that initiating or completing the registration (for example, via the registration and installation wizard) would also equate “receiving... a request from [the] owner... to register” the laptop, as discussed in connection with limitation 1[c][i]. *See, e.g.*, EX1019, 2-3; EX1003, ¶232. Thus, zTrace renders this limitation obvious.

**(c) Limitation 9[b]**

This limitation is an obvious extension of limitation 9[a] and an obvious next step of requesting registration of the laptop from the zTrace™ service. EX1003, ¶¶233-234. For example, in the case where an owner wants to register a new laptop with the zTrace™ service, zTrace instructs to “[j]ust resubmit your registration, and your new computer will be zTrace™ protected too.” EX1019, 3. The submission

here acts as the “**request**” and the subsequent laptop protection is what happens after “**registering the mobile device with the security service.**” EX1003, ¶233. Similarly, as discussed for limitation 1[c][i], completing the “registration and installation wizard” on the laptop would predictably result in the laptop being registered with the system. EX1019, 2; EX1007; EX1003, ¶234.

For these reasons, zTrace in view of Kesler, Isikoff and/or Bonnett render independent claim 9 obvious.

### **3. Dependent claims 7 and 15**

Claim 7 depends from claim 1 and claim 15 depends from claim 9. zTrace instructs that “[i]f your computer is out of your direct control, make the data invisible, encrypt it, recover it and then delete it.” EX1005. Thus, zTrace discloses that files and data are first “**copied**” (i.e., recovered) from the laptop and then “**deleted**” from the laptop. *See* limitation 1[c][vi] (addressing copying user data to the zServer); EX1003, ¶237.

This same sequence can be implemented when predefined actions are executed. *See* limitation 1[c][vi] above; EX1003, ¶238. “Predefined actions can include retrieving files [and] deleting sensitive user information[.]” EX1013. zTrace instructs laptop owners to “[d]ecide which files and directories are critical and define actions you want to occur if the computer falls out of your control.” *Id.*

With respect to claim 7, which further requires that “**the security application... perform**” the deleting, zTrace makes clear that the zControl application performs this function on the laptop. *See, e.g.*, EX1053 (“zControl... deletes sensitive information”); EX1026; EX1028; EX1013; EX1003, ¶239.

Thus, dependent claims 7 and 15 are disclosed or rendered obvious by zTrace alone or the combination of zTrace and Isikoff.

**C. Ground 2: Claims 1, 7, 9 and 15 are rendered obvious by zTrace in view of Kesler, Isikoff and Eckardt**

For **Ground 2**, Petitioners replace Bonnett with Eckardt to render limitations 1[d]-1[g] and 9[h]-9[k] obvious. Eckardt is a patent assigned to Intel describing hidden disk partition features that would have been implemented in zTrace’s hard drive and executed by zTrace’s Intel 386™ DX processor. Eckardt, cover at (73); EX1019, 2 (zTrace “run[s] on Desktop and Laptop Computers with... 386 DX or higher”); EX1035, 1; EX1003, ¶241. All other arguments under **Ground 1** remain the same and are incorporated by reference into **Ground 2**.

**1. Limitation 1[d]**

As discussed for limitation 1[d] under **Ground 1**, zTrace discloses a hard drive that is the claimed “**non-volatile memory.**” *See* EX1019, 2; EX1036, 56; EX1037, 481; EX1001, 22:13-18; EX1003, ¶242.

## 2. Limitation 1[e]

This limitation is rendered obvious by the combined disclosures of zTrace and Eckardt. As discussed for limitation 1[e] under **Ground 1**, zTrace provides ample disclosures suggesting that the zTrace Gold and zControl applications are stored in a secure area (i.e., a “**system area**”) on the hard drive. *See* EX1007; EX1019, 2-3; EX1013; EX1026; EX1053; EX1003, ¶¶243-244. But zTrace falls short of affirmatively identifying those hidden or secure areas. Eckardt, however, provides these disclosures.

Eckardt discloses a hard drive with a “legal” partition and an “illegal” partition. The “legal” partition is recognizable by the operating system and “fully accessible by the user” after the boot sequence. Eckardt, 1:22-33, 4:41-59, claims 1, 4, 6. This partition acts as the claimed “**changeable area that can be modified by the user.**” EX1003, ¶¶244-245. The “illegal” partition in Eckardt is not recognizable by the operating system and “cannot be read or modified” after the boot sequence. Eckardt, 3:8-14, 3:30-45, 4:35-38, 4:51-59, 5:7-18 (“after boot, [the] hidden partition will not be accessible”), FIG. 1, claims 1, 4, 6. The “illegal” partition – also referred to as “a hidden disk area” in Eckardt – can include “programs that the end user must not modify in any way.” Eckardt, 1:42-46. This partition acts as the claimed “**system**

**area that cannot be modified by the user.”**<sup>5</sup> EX1003, ¶245.

It would have been obvious to combine the general teachings of Eckardt with zTrace, predictably resulting in the laptop’s hard drive being partitioned to include a hidden disk area (“**system area**”) and an area that is accessible to the user (“**changeable area**”). EX1003, ¶¶246-251. zTrace’s disclosures provide the teaching, suggestion and motivation for this combination and hard drive configuration. EX1003, ¶246. Eckardt confirms that “hard disks... are often ‘partitioned’ into multiple logical subdivisions.” Eckardt, 1:10-16. And in its background discussion, further confirms that the “legal” and “illegal” partitions were well known in the art prior to its 1999 filing date. Eckardt, 1:10-57. A POSITA would have therefore understood how to implement these partitions in zTrace’s hard drive with a reasonable expectation of success. EX1003, ¶247. It also would have been obvious to try combining zTrace with Eckardt for the same reasons. *Id.*

A POSITA would have been motivated to seek more information about how

---

<sup>5</sup> This interpretation of the “**changeable area**” and the “**system area**” is consistent with PO’s application of these claim terms in its infringement contentions in the parallel district court litigation, as discussed above for limitation 1[e] under **Ground 1**.

to implement hidden areas within the hard drive to keep the zTrace applications “invisible” to the end user. EX1003, ¶248. A POSITA would have been particularly motivated to look to Eckardt for these details because it is a patent from Intel and, as discussed for limitation 1[a] under **Ground 1**, the zTrace laptop includes a 386™ DX processor by Intel. Eckardt, (73); EX1019, 2; EX1035, 1. A POSITA would have understood that the functionality of these Intel-based components would have complemented each other and there would have been a reasonable expectation of success in combining them. EX1003, ¶248.

For the same reasons discussed for this limitation under **Ground 1**, a POSITA would have recognized the benefit of partitioning the hard drive in zTrace to include a hidden partition that cannot be accessed by the end user. *See* Bonnett, [0011] (“Restricting access to programs and/or portions of a program can help prevent a user from deleting or corrupting those portions of the program, which can lead to an improved reliability of the [device]”), [0037]; EX1003, ¶249.

With respect to Kesler and Isikoff, these references are also in the computer arts and involve concealing software from unauthorized device users and are therefore complementary references to Eckardt. Kesler, [0015]; Isikoff, 1:59-65. Kesler describes embodiments of zTrace™ so a POSITA would be motivated to combine Kesler with Eckardt for the same reasons discussed for zTrace. Kesler,

[0017]; EX1003, ¶250. Isikoff is relied on for the limited purposes of teaching disabling laptop features and copying data from the laptop to the server for recovery purposes, neither of which would be impacted by implementing hidden partitions in the zTrace laptop. EX1003, ¶250.

For these reasons, the combination of zTrace and Eckardt renders this limitation obvious.

### **3. Limitation 1[f]**

This limitation is also rendered obvious by the combination of zTrace and Eckardt. As discussed for limitation 1[c] under **Ground 1**, the zTrace Gold application is installed on the hard drive and it would have been obvious for the zControl application to be installed at the same location. *See supra*. As just discussed for limitation 1[e] under **Ground 2**, zTrace suggests that these applications are in hidden areas within the hard drive, which makes them “invisible” or “undetectable” to the laptop user. *See* EX1007; EX1013; EX1026; EX1053; EX1019, 2-3. Thus, the combined prior art renders obvious that “**the security application utilizes code residing at least partially in the system area**” because the applications themselves reside in the hidden area on the hard drive in zTrace. EX1003, ¶252.

### **4. Limitation 1[g]**

As discussed for limitations 1[c][iv] and 1[g] under **Ground 1**, zTrace alone or in combination with Kesler and/or Isikoff discloses that “**the security application**

**receives the notification from at least one of the servers.”** As also discussed for limitation 1[g] under **Ground 1**, the ’649 patent disclosures and PO’s application of the **“via the system area”** element in the parallel district court litigation indicate that this element is satisfied by any security software residing in a secure area (i.e., the **“system area”**) that receives notifications from a server. *See* EX1001, 20:8-31, FIG. 48, 19:8-26, FIG. 45, 33:24-34:46; EX1036, 72.

When zTrace is modified by Eckardt, the zTrace Gold and zControl applications reside in a hidden partition of the laptop’s hard drive (as discussed for limitation 1[f] under **Ground 2**) and these applications receive notifications from the zServer (as discussed for limitation 1[c][iv] under **Ground 1**). Thus, consistent with PO’s interpretation of this claim limitation, a POSITA would have understood that these applications receive the notification from the zServer **“via the system area.”** EX1003, ¶¶253-254. Limitation 1[g] is thus satisfied.

Alternatively, in light of zTrace’s and Eckardt’s teaching, a POSITA would have known it was an obvious design choice for the security application to receive notifications from a security server **“via the system area”** because it would promote zTrace’s and Eckardt’s express teachings to prevent thieves from thwarting the operation of the security system by concealing the application and preventing its modification or removal, which would extend to functionality for communicating

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

with a security server. *See* Eckardt, 1:35-50, 4:52-59; EX1007; EX1013; EX1026; EX1053; EX1019, 2-3; Kesler, [0009], [0017]; EX1003, ¶255.

For these reasons, independent claim 1 is rendered obvious by zTrace in view of Kesler, Isikoff and/or Eckardt under **Ground 2**. Independent claim 9 is rendered obvious for the same reasons as claim 1 under **Ground 2**. Dependent claims 7 and 15 are obvious for the same reasons discussed under **Ground 1**.

## **VIII. SECONDARY CONSIDERATIONS**

PO has not provided any meaningful argument or evidence of secondary considerations in the parallel district court litigation. It responded to an interrogatory for secondary consideration information with high-level, generic statements without specifically identifying products or a nexus to the claim language. EX1056, 20-21. Regardless, there are no secondary considerations that would weigh against the strong showing of obviousness demonstrated above. EX1003, ¶257.

## **IX. CONCLUSION**

Petitioner respectfully requests institution of IPR based on the grounds set forth and described above.

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

Dated: December 11, 2023

Respectfully submitted,

COOLEY LLP  
ATTN: Patent Group  
1299 Pennsylvania Avenue NW  
Suite 700  
Washington, DC 20004  
Tel: (650) 843-5001  
Fax: (650) 849-7400

By: /Heidi L. Keefe/  
Heidi L. Keefe  
Reg. No. 40,673  
Counsel for Petitioner

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

**CERTIFICATE OF COMPLIANCE WITH WORD COUNT**

Pursuant to 37 C.F.R. § 42.24(d), I certify that this petition complies with the type-volume limits of 37 C.F.R. § 42.24(a)(1)(i) because it contains 13,794 words, according to the word-processing system used to prepare this petition, excluding the parts of this petition that are exempted by 37 C.F.R. § 42.24(a) (including the table of contents, a table of authorities, mandatory notices, a certificate of service or this certificate word count, appendix of exhibits, and claim listings).

DATED: December 11, 2023

COOLEY LLP  
ATTN: Patent Group  
1299 Pennsylvania Avenue,  
NW Suite 700  
Washington, D.C. 20004  
Tel: (650) 843-5001  
Fax: (650) 849-7400

/Heidi L. Keefe/  
Heidi L. Keefe  
Reg. No. 40,673

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

**CERTIFICATE OF SERVICE**

I hereby certify, pursuant to 37 C.F.R. Sections 42.6 and 42.105, that a complete copy of the attached **PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,506,649 B2**, including all exhibits (**Nos. 1001-1058**) and related documents, are being served via Federal Express on the 11<sup>th</sup> of December, the same day as the filing of the above-identified document in the United States Patent and Trademark Office/Patent Trial and Appeal Board, upon Patent Owner by serving the correspondence address of record with the USPTO as follows:

GEORGIOS GEORGAKIS  
**138358 - G+J Softex Temp**  
4301 W WILLIAM CANNON DR  
STE B150 PMB 200  
AUSTIN, TX 78749-1487  
UNITED STATES

And, via Federal Express upon counsel of record for Patent Owner in the litigation pending before the U.S. District Court for the Western District of Texas entitled *Softex LLC v. Absolute Software Corp.*, Case No. 1:22-cv-01308-DAE (W.D. Tex.) as follows:

Blair M. Jacobs  
Christina A. Ondrick  
John S. Holley  
**MCKOOL SMITH, P.C.**  
1999 K Street, NW Suite 600  
Washington, D.C. 20006

John B. Campbell  
**MCKOOL SMITH, P.C.**  
303 Colorado Street, Suite 2100  
Austin, TX 78701

Casey L. Shomaker  
Matthew Folks  
Joseph Micheli  
**MCKOOL SMITH, P.C.**  
300 Crescent Court, Suite 1500  
Dallas, TX 75201

Petition for *Inter Partes* Review of  
U.S. Patent No. 8,506,649 B2

DATED: December 11, 2023

/Heidi L. Keefe/  
Heidi L. Keefe  
Reg. No. 40,673

# APPENDIX A

Appendix A  
Claims 1, 7, 9, 15  
U.S. Patent No. 8,506,649

| Claim Limitations |                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.[pre]           | A mobile electronic device, comprising:                                                                                                                                                                                                                                                                                                                       |
| 1[a]              | a processor;                                                                                                                                                                                                                                                                                                                                                  |
| 1[b]              | one or more non-transitory machine-readable storage media responsive to the processor; and                                                                                                                                                                                                                                                                    |
| 1[c]              | a security application in at least one of the non-transitory machine-readable storage media, wherein the security application is operable to perform operations comprising:                                                                                                                                                                                   |
| 1[c][i]           | enabling an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers;                                                                                                                                                                                        |
| 1[c][ii]          | causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;                                                                                                                                                                                                                  |
| 1[c][iii]         | after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to periodically communicate with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;                                                   |
| 1[c][iv]          | after the owner has registered the mobile electronic device with the security service, accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device; |
| 1[c][v]           | in response to receiving the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and                                                                                                                                 |
| 1[c][vi]          | automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;                                                                                                                                                                                                                                  |
| 1[d]              | wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;                                                                                                                                                                                                                                                          |
| 1[e]              | wherein the non-volatile memory comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user;                                                                                                                                                                                                             |

|                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1[f] wherein the security application utilizes code residing at least partially in the system area; and                                                                                                                                                                                                                                                  |
| 1[g] wherein the security application receives the notification from at least one of the servers via the system area.                                                                                                                                                                                                                                    |
| 7. A mobile electronic device according to claim 1, wherein the operations the security application is operable to perform further comprise: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device. |
| 9.[pre] A method for providing security for a mobile electronic device, the method comprising:                                                                                                                                                                                                                                                           |
| 9[a] receiving, at a mobile electronic device, a request from an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers;                                                                                                                              |
| 9[b] in response to the request from the owner, registering the mobile electronic device with the security service;                                                                                                                                                                                                                                      |
| 9[c] automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;                                                                                                                                                                                                           |
| 9[d] after the owner has registered the mobile electronic device with the security service, periodically communicating with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;                                                                               |
| 9[e] after the owner has registered the mobile electronic device with the security service, accepting a notification from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device;                       |
| 9[f] in response to accepting the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and                                                                                                                       |
| 9[g] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;                                                                                                                                                                                                                        |
| 9[h] wherein the mobile electronic device comprises non-volatile memory;                                                                                                                                                                                                                                                                                 |
| 9[i] wherein the non-volatile memory comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user;                                                                                                                                                                                                   |
| 9[j] wherein the security application utilizes code residing at least partially in the system area; and                                                                                                                                                                                                                                                  |

9[k] wherein the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via the system area.

15. A method according to claim 9, further comprising: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.