

Declaration of Dr. Polish in Support of
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 CORPORATION and ABSOLUTE SOFTWARE,
INC.,
Petitioners

v.

SOFTEX LLC,
Patent Owner

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

Title: ELECTRONIC DEVICE SECURITY AND TRACKING SYSTEM AND METHOD

DECLARATION OF DR. NATHANIEL POLISH

TABLE OF CONTENTS

	Page
I. INTRODUCTION AND QUALIFICATIONS.....	3
A. Qualifications and Experience	3
B. Materials Considered.....	6
II. PERSON OF ORDINARY SKILL IN THE ART	13
III. STATEMENT OF LEGAL PRINCIPLES.....	14
A. Prior Art.....	15
B. Claim Construction	15
C. Legal Standards for Obviousness.....	17
IV. TECHNOLOGY BACKGROUND.....	23
A. Security for Mobile Devices	23
B. Memory Partitions.....	23
V. THE '649 PATENT	27
A. Priority Date	27
B. Overview of the Specification.....	27
VI. APPLICATION OF THE PRIOR ART TO THE CHALLENGED CLAIMS	30
A. Brief Summary of Prior Art	31
1. zTrace [EX1004-EX1028, EX1052-EX1053].....	31
2. Kesler [EX1029]	41
3. Isikoff [EX1030]	45
4. Bonnett [EX1031]	47
5. Eckardt [EX1032]	48
A. Ground 1: Claims 1, 7, 9 and 15 are rendered obvious by zTrace in view of Kesler, Isikoff and Bonnett.	49

TABLE OF CONTENTS

(continued)

	Page
1. Independent claim 1	49
2. Independent claim 9	135
3. Dependent claims 7 and 15	141
B. Ground 2: Claims 1, 7, 9 and 15 are rendered obvious by zTrace in view of Kesler, Isikoff and Eckardt	143
1. Limitation 1[d]: “wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;”	144
2. Limitation 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;”	144
3. Limitation 1[f]: “wherein the security application utilizes code residing at least partially in the system area; and”	149
4. Limitation 1[g]: “wherein the security application receives the notification from at least one of the servers via the system area.”	150
VII. NO SECONDARY CONSIDERATIONS OF NONOBVIOUSNESS.....	152
VIII. CONCLUSION.....	154

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

I, Dr. Nathaniel Polish, declare as follows:

I. INTRODUCTION AND QUALIFICATIONS

A. Qualifications and Experience

1. I am an independent consultant. All of my opinions stated in this report are based on my own personal knowledge and professional judgment. In forming my opinions, I have relied on my knowledge and experience in computer technology, computer networking, computer security, and mobile networking.

2. I am over 18 years of age and, if I am called upon to do so, I would be competent to testify as to the matters set forth herein. A copy of my current curriculum vitae, which details my education and professional and academic experience, is included as **Appendix A** to this declaration. The following provides an overview of some of my experience that is relevant to the matters set forth in this declaration.

3. I expect to testify regarding my background, qualifications, and experience relevant to the issues in this litigation. I have a Ph.D. in Computer Science from Columbia University. I hold the following four degrees from Columbia, spanning the years 1980 to 1993:

- Ph.D. in Computer Science, May 1993, Thesis: Mixed Distance

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Measures for the Optimization of Concatenative Vocabularies in
Speech Synthesis;

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

4. For over thirty years, I have run a computer technology development firm that I co-founded, called Daedalus Technology Group. My primary business activity is the development of computer-related products. This activity involves understanding the business objectives of customers, designing products to suit their needs, and supervising the building, testing, and deployment of these products. I develop hardware and software as well as supervise others who do so.

5. In 2019, I founded a company called SuperAlert. I am the CEO of that company. I am the main product developer for SuperAlert. SuperAlert is in the business of building and deploying wireless sensors for monitoring systems in large residential buildings. These systems include heating systems, pumps, and hot water heaters. SuperAlert products utilize low power long range radio signals. SuperAlert uses complex networking approaches that allow the sensors to reliably and securely communicate with databases, websites, servers, and end user devices.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

6. Also, from time to time I found other companies in order to pursue particular product opportunities. I develop and ultimately sell these companies. Most of my business activity, however, is as a consulting product developer. From time to time I have also served as an expert witness on computer and software related cases. I am a named inventor on eight United States patents and am a member of several professional societies, including the IEEE and ACM.

7. I have extensive experience in several areas relevant to this case. I have worked for many years on products that utilize digital wireless data transmission. I have worked on projects that use VPNs and well as modified protocol stacks to achieve their purposes. Many of those concepts are very similar to the technologies involved in this matter.

8. In the 1990s, I developed many a product for a company called burst.com that delivered digital audio and video to end users on the internet. There was at least one version of that product that used a modified TCP/IP stack to improve performance under special network conditions. Modification of the network protocol stack is a technique that I have experience with.

9. In the 1990s as well, I had experience designing and building applications that managed secure transactions over public computer networks. One such example was for a company known as OneClickCharge that was implementing

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

a secure micropayment and media delivery system.

10. In the early 2000s, I worked with a company called Allure to develop a document beaconing technology. This technology sent a network-based beacon whenever certain documents were opened by a user. This technology was used to document authorized and unauthorized document usage.

11. Through these and other experiences, I am very familiar with the technologies at issue in this matter.

B. Materials Considered

12. The analysis that I provide in this Declaration is based on my education, research, and experience, as well as the documents I have considered. In forming my opinions, I have read and considered U.S. Patent No. 8,506,649 B2 (“’649 patent”) [EX1001] and its prosecution history [EX1002]. I have cited to or considered the following documents in my analysis below:

Exhibit 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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Exhibit No.	Description of Document
1004	zTrace Overview page: https://web.archive.org/web/20020802143350/http://www.ztrace.com:80/
1005	zTrace zSecurity Suite page: https://web.archive.org/web/20020604051951/http://www.ztrace.com:80/zSecuritySuite.asp
1006	zTrace Gold page: https://web.archive.org/web/20020810160306/http://www.ztrace.com:80/zTraceGold.asp
1007	zTrace Gold Brochure: https://web.archive.org/web/20030319061040/http://ztrace.com/data_sheet/zTraceGold.pdf
1008	zTrace zPass page: https://web.archive.org/web/20020604052039/http://www.ztrace.com:80/zPass.asp
1009	zTrace zPass Brochure: https://web.archive.org/web/20030510220600/http://www.ztrace.com/data_sheet/zPass.pdf
1010	zTrace zEncrypt:

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

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

Declaration of Dr. Polish in Support of
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: https://web.archive.org/web/20020613175056/http://www.ztrace.com/zAssetTrackWhy.asp
1018	zTrace – Why You Need zTrace page: https://web.archive.org/web/20020613180259/http://www.ztrace.com:80/zTraceWhy.asp
1019	zTrace – FAQ page: https://web.archive.org/web/20020405211735/http://www.ztrace.com:80/faq.asp
1020	zTrace – zGuarantee page: https://web.archive.org/web/20021002045822/http://www.ztrace.com:80/guarantee.asp
1021	zTrace – Corporate page: https://web.archive.org/web/20020606100347/http://www.ztrace.com/Corporate.asp
1022	zTrace – How zTrace Works page: https://web.archive.org/web/20020814065623/http://www.ztrace.com:80/zTraceHow.asp
1023	zTrace – About zTrace page: https://web.archive.org/web/20020604025540/http://www.ztrace.com:80/AboutzTrace.asp

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Exhibit No.	Description of Document
1024	zTrace – Press Release re zTrace Security Suite: https://web.archive.org/web/20021019100311/http://www.ztrace.com/pr_releases/HpEducational.pdf
1025	zTrace – 2003 Press Releases page: https://web.archive.org/web/20030820024638/http://www.ztrace.com:80/PressReleases.asp
1026	zTrace – Press Release re zControl: https://web.archive.org/web/20040518054736/http://www.ztrace.com/pr_releases/zControl.pdf
1027	zTrace – 2004 Press Releases page: https://web.archive.org/web/20040226194817/http://ztrace.com/PressReleases.asp
1028	zTrace – Press Release for Yale University and zTrace Partnership: https://web.archive.org/web/20040531010618/http://www.ztrace.com/pr_releases/Yale.pdf
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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Exhibit No.	Description of Document
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)
1038	Excerpts from Terry William Ogletree et al., Windows XP Unleashed (2002)
1039	U.S. Patent No. 6,300,863 issued to Christian Cotichini et al. (filed Mar. 24, 1998, issued Oct. 9, 2001) ("Cotichini")
1040	U.S. Patent No. 10,257,551 B2 issued to Leslie L. Grandy et al. (filed Dec. 12, 2016, issued Apr. 9, 2019) ("Grandy")
1041	U.S. Patent No. 6,775,828 B2 issued to David Feinleib et al. (filed July 19, 1999, issued Aug. 10, 2004) ("Feinleib")
1042	U.S. Patent No. 7,716,719 B2 issued to Victor Kouznetsov et al. (filed Apr. 21, 2005, issued May 11, 2010) ("Kouznetsov")
1043	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")
1044	Excerpts from Douglas Comer, Operating System Design, The Xinu Approach, Linksys Version (2012) ("Comer")
1045	Herb Goronkin & Yang Yang, <i>High-Performance Emerging Solid-State Memory Technologies</i> , MRS Bulletin, 806-813 (Nov. 2004) ("Goronkin")
1046	Roberto Bez et al., <i>Introduction to Flash Memory</i> , Proceedings of the IEEE, 91(4):489-502 (Apr. 2003) ("Bez")
1047	U.S. Patent No. 5,852,306 issued to Leonard Forbes (filed Jan. 29, 1997, issued Dec. 22, 1998) ("Forbes")
1048	Excerpts from Andrew S. Tanenbaum, Operating Systems: Design and Implementation (1987)

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Exhibit No.	Description of Document
1049	U.S. Patent No. 5,537,540 issued to Craig A. Miller et al. (filed Sept. 30, 1994, issued July 16, 1996) (“Miller”)
1050	U.S. Patent No. 6,725,178 B2 issued to Richard W. Cheston et al. (filed Jan. 15, 2002, issued Apr. 20, 2004) (“Cheston”)
1051	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”)
1052	zTrace – Protect, Monitor, Recover: https://web.archive.org/web/20030811214545/http://www.ztrace.com:80/home_ie.asp
1053	zTrace – zControl Maintains data privacy after computer loss: https://web.archive.org/web/20030811223300/http://www.ztrace.com:80/zControl.asp
1054	Edward C. Baig, <i>Unlock the secrets of security for your laptop</i> , USA Today, April 9, 2002, https://web.archive.org/web/20060504120338/http://www.usatoday.com:80/tech/columnist/2002/04/10/baig.htm
1055	Yahoo Internet Life Magazine, <i>URL Guide</i> , zTrace.com (July 2002), https://web.archive.org/web/20021025034410/http://www.ztrace.com/sites/yahoo50/yil.com.html
1056	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.)
1057	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)
1058	Affidavit of Nathaniel E Frank-White, dated November 16, 2023

II. PERSON OF ORDINARY SKILL IN THE ART

13. I am informed by counsel that, under the patent laws in effect before the America Invents Act (“AIA”) of 2011, an assessment of claims of a patent filed before the AIA took effect should be undertaken from the perspective of a person of ordinary skill in the art as of the earliest claimed priority date (i.e., the “time the invention was made”), which I have assumed is August 23, 2003.

14. Counsel has advised me that to determine the appropriate level of one of ordinary skill in the art, I may consider the following factors: (a) the types of problems encountered by those working in the field and prior art solutions thereto; (b) sophistication of the technology in question, and the rapidity with which innovations occur in the field; (c) the educational level of active workers in the field; and (d) the educational level of the inventor.

15. The relevant technical field for the ’649 patent is security software for mobile devices. Based on this, and the four factors above, in my opinion a POSITA as of August 2003 would have had at least an undergraduate degree in computer science (or equivalent degree) and one to two years of experience developing security-related software for mobile devices and would further have familiarity with non-volatile memories. This definition is approximate, and more experience may substitute for education or vice versa.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

16. My opinions regarding the level of ordinary skill in the art are based on, among other things, my over thirty years of experience in the relevant areas, my understanding of the basic qualifications that would be relevant to an individual tasked with investigating the methods and devices in the relevant areas, and my familiarity with the backgrounds of researchers and practitioners in the related areas, including colleagues, students, and other individuals, both past and present, who work in these areas.

17. Although my qualifications and experience exceed those of the hypothetical person having ordinary skill in the art defined above, my analysis and opinions regarding the '649 patent have been based on the perspective of a person of ordinary skill in the art in August 2003.

18. My opinions herein regarding the understanding of a person of ordinary skill in the art and my other opinions set forth herein would remain the same if the person of ordinary skill in the art were determined to have somewhat more or less education and/or experience than I have identified above.

III. STATEMENT OF LEGAL PRINCIPLES

19. I am not a patent attorney, nor have I independently researched the law on patent validity. Attorneys for Petitioner explained certain legal principles to me

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

that I have relied upon in forming my opinions set forth in this report.

A. Prior Art

20. I understand that the law provides categories of information that constitute prior art that may be used to anticipate or render obvious patent claims. To be prior art to a particular patent under the relevant law, references must have been made, known, used, published, or patented, or be the subject of a patent application by another, before the priority date of the patent. I also understand that the POSA is presumed to have knowledge of the relevant prior art.

21. I have assumed for purposes of this Declaration that claims 1, 7, 9 and 15 of the '649 patent are entitled to an August 23, 2003 priority date. I reserve the right to update my analysis (or to determine that my analysis does not require updating) should Patent Owner later attempt to prove an earlier date of conception and attempt to establish that the '649 patent is entitled to an earlier priority date.

B. Claim Construction

22. I understand that under the relevant legal principles, claim terms are generally given their ordinary and customary meaning, which is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application. I further understand that the person of ordinary skill in the art is deemed to read the claim

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

term not only in the context of the particular claim in which a claim term appears, but in the context of the entire patent, including the specification.

23. I am informed by counsel that the patent specification, under applicable legal principles, has been described as the single best guide to the meaning of a claim term, and is thus highly relevant to the interpretation of claim terms. And I understand for terms that do not have a customary meaning within the art, the specification usually supplies the best context of understanding the meaning of those terms.

24. I am further informed by counsel that other claims of the patent in question, both asserted and unasserted, can be valuable sources of information as to the meaning of a claim term. Because the claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims. Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.

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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

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

27. I have been instructed by counsel to apply the “*Phillips*” claim construction standard for purposes of interpreting the claims in this proceeding, to the extent they require an explicit construction. The description of the legal principles set forth above provides my understanding of the “*Phillips*” standard as provided to me by counsel. I have interpreted all the claim terms in accordance with the ordinary and customary meaning of such terms as understood by one of ordinary skill in the art in August 2003.

C. Legal Standards for Obviousness

28. I have been provided the following instructions from the Federal Circuit Bar Association Model Instructions regarding obviousness, which I reproduced in part below. I apply this understanding in my analysis, with the caveat that I have

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

been informed that the Patent Office will find a patent claim invalid in *inter partes* review if it concludes that it is more likely than not that the claim is invalid (*i.e.*, a preponderance of the evidence standard), which is a lower burden of proof than the “clear and convincing” standard that is applied in United States district court (and described in the jury instruction below):

4.3c OBVIOUSNESS

Even though an invention may not have been identically disclosed or described before it was made by an inventor, in order to be patentable, the invention must also not have been obvious to a person of ordinary skill in the field of technology of the patent [at the time the invention was made] or [before the filing date of the patent].

[Alleged infringer] may establish that a patent claim is invalid by showing, by clear and convincing evidence, that the claimed invention would have been obvious to persons having ordinary skill in the art at the time the [invention was made] or [patent was filed] in the field of [insert the field of the invention].

In determining whether a claimed invention is obvious, you must consider the level of ordinary skill in the field

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

[of the invention] that someone would have had at the time the [invention was made] or [patent was filed], the scope and content of the prior art, and any differences between the prior art and the claimed invention.

Keep in mind that the existence of each and every element of the claimed invention in the prior art does not necessarily prove obviousness. Most, if not all, inventions rely on building blocks of prior art. In considering whether a claimed invention is obvious, you may but are not required to find obviousness if you find that at the time of the claimed invention [or the patent's filing date] there was a reason that would have prompted a person having ordinary skill in the field of [the invention] to combine the known elements in a way the claimed invention does, taking into account such factors as (1) whether the claimed invention was merely the predictable result of using prior art elements according to their known function(s); (2) whether the claimed invention provides an obvious solution to a known problem in the relevant field; (3) whether the prior art teaches or suggests the desirability of combining elements claimed in the invention; (4) whether the prior art teaches away from combining elements in the claimed invention; (5) whether it would have been obvious to try

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

the combinations of elements, such as when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions; and (6) whether the change resulted more from design incentives or other market forces. To find it rendered the invention obvious, you must find that the prior art provided a reasonable expectation of success. Obvious to try is not sufficient in unpredictable technologies.

In determining whether the claimed invention was obvious, consider each claim separately. Do not use hindsight, i.e., consider only what was known at the time of the invention [or the patent's filing date].

In making these assessments, you should take into account any objective evidence (sometimes called "secondary considerations") that may shed light on the obviousness or not of the claimed invention, such as:

- (a) Whether the invention was commercially successful as a result of the merits of the claimed invention (rather than the result of design needs or market-pressure advertising or similar activities);
- (b) Whether the invention satisfied a long-felt need;

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

- (c) Whether others had tried and failed to make the invention;
- (d) Whether others invented the invention at roughly the same time;
- (e) Whether others copied the invention;
- (f) Whether there were changes or related technologies or market needs contemporaneous with the invention;
- (g) Whether the invention achieved unexpected results;
- (h) Whether others in the field praised the invention;
- (i) Whether persons having ordinary skill in the art of the invention expressed surprise or disbelief regarding the invention;
- (j) Whether others sought or obtained rights to the patent from the patent holder; and
- (k) Whether the inventor proceeded contrary to accepted wisdom in the field.

Federal Circuit Bar Association Model Patent Jury Instructions §4.3c (2014).

29. I am also informed that the United States Patent Office supplies its examining corps with a Manual of Patent Examining Procedure that provides

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

exemplary rationales that may support a conclusion of obviousness, including:

- (A) Combining prior art elements according to known methods to yield predictable results;
- (B) Simple substitution of one known element for another to obtain predictable results;
- (C) Use of known technique to improve similar devices (methods, or products) in the same way;
- (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- (E) “Obvious to try” – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art;
- (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

the prior art reference or to combine prior art reference
teachings to arrive at the claimed invention.

Manual of Patent Examining Procedure, §2143 (9th ed. Mar. 2014), E9R-11.2013.

I apply these principles in my analysis below.

IV. TECHNOLOGY BACKGROUND

A. Security for Mobile Devices

30. The portability and convenience offered by mobile devices is offset by the fact that they are especially susceptible to theft. EX1039 [Cotichini], 1:20-25. Theft of mobile devices not only means a loss of an expensive piece of equipment, but also the loss of sensitive business or personal information stored on the device itself. EX1029 [Kesler], [0003]. The increasing prevalence of mobile devices has led to great interest in data recovery and protection technologies. EX1039 [Cotichini], 1:20-25. Over the last 20 years, skilled artisans and technology companies have invested time and resources to develop better ways of preventing mobile device theft, including tracing stolen devices for device or data recovery. *See* EX1029 [Kesler], [0003]; EX1030 [Isikoff], Abstract; EX1039 [Cotichini], 1:26-34.

B. Memory Partitions

31. In the context of computer operating systems, “memory” is well

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

understood as “[t]he part of a computer or sophisticated phone system which stores information or instructions for use.” EX1037, 433. Memory comes in many variations, such as random-access memory (RAM) or hard disk (HD or SSD). *Id.*, 433, 481; EX1044 [Comer], 371.¹ A person of ordinary skill in August 2003 would have known that these different variations of memory could be segmented into areas that would have different levels of privileges associated with them. EX1038, 12.

32. In the case of RAM, it is well known in common operating systems that memory is sectioned into system and user spaces. EX1044 [Comer], 35-36, Fig. 3.3; EX1048 [Tanenbaum], 196. System spaces are only accessible to privileged parts of the operating systems known generally as the kernel and non-system user spaces are accessible to ordinary applications. EX1044 [Comer], 45; EX1048 [Tanenbaum], 197; EX1038, 12. Often those user spaces are themselves sectioned to be accessible to only certain applications. EX1048 [Tanenbaum], 197; EX1049 [Miller], 15:26-37 (“The user cannot inadvertently delete or alter the detection software... [n]or can a virus access the partition.”). These concepts have been taught in undergraduate

¹ I note that the Comer textbook has a publication date later than August 2003. However, the content I rely on in this textbook was well known prior to August 2003.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

computer science classes since at least the 1980s. EX1048 [Tanenbaum], 3.

33. In the case of HDs, it is well known in operating systems that drives are divided into different sections called “partitions.” EX1032 [Eckardt], 1:10-14 (“Certain hard disks, including a hard disk on a personal computer, are often ‘partitioned’ into multiple logical sub-divisions. Each partition is essentially a separate portion of the disk, which is addressed and handled separately from the other partitions.”). There are sections that are left out of the partitioning, and are therefore not normally visible to user programs. EX1044 [Comer], 45. Track zero is one such section. *See* EX1032 [Eckardt], 2:60-67; EX1029 [Kesler], [0017]. The partitions are usually further controlled so that only certain users or programs can access them. EX1032 [Eckardt], 1:42-46. This can be for security reasons or to prevent a malfunctioning program from overwriting or modifying them. EX1032 [Eckardt], 1:42-46. These partitions are generally controlled by a partition table and managed by a partition manager. One such example of a partition manager is fdisk in some versions of Windows and Unix.

34. Flash memory was in wide distribution by 2003. EX1031 [Bonnett], [0031]. Flash memory is a semiconductor memory that, when written to, will retain the data until explicitly erased. EX1044 [Comer], 140. It is therefore non-volatile memory that can be read from even when power is lost. EX1037, 481. Usually,

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

flash memory can be as fast as RAM for reading but is quite slow when written to. EX1046 [Bez], 490; EX1045 [Goronkin], 807.² In this time frame, flash would typically be used as a replacement for hard drives. EX1046 [Bez], 490; EX1047 [Forbes], 1:35-44.

35. It has been a common approach in security applications for many years prior to 2003 to create partitions that are not typically visible to the operating system. Bonnett, [0036] (“hidden partition 206*b* operates to store at least a portion 225*b* of program 225 that a program designer desires to be made inaccessible to a user of appliance 200.”); Cheston, 2:16-19 (“[T]he hidden partition is preferably inaccessible to the operating system thereby decreasing the probability of code stored therein being corrupted”). These hidden partitions are used to hide sensitive data from ordinary programs or users. Dayan, [0008] (“The designated partition may be invisible to the operating system and resistant to modification by any programs running under the operating system.”).

² I note that the Goronkin paper has a publication date later than August 2003. However, the content I rely on in this paper was well known prior to August 2003.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

V. THE '649 PATENT

A. Priority Date

36. The '649 patent, which was filed on July 11, 2006, purports to claim priority back to a provisional application filed on August 23, 2003. I understand that Petitioners are not challenging this date for purposes of this Petition.

B. Overview of the Specification

37. The '649 patent describes an “electronic device security and tracking system and method,” referred to throughout the specification as “ESTSM.” EX1001, 1:36-2:15. In my opinion, this ESTSM is nothing new, as each of the key elements, including those recited in the claims, were well known in the art at the time of the '649 patent's earliest purported priority date (August 23, 2003).

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

38. The ESTSM “includes a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with [a] stolen electronic device.” *Id.* The specification discloses that software is pre-installed on an electronic device so that “upon first time power-on and connection to the ESTSM server” “the user is prompted to register for different ESTSM services.” *Id.*; *see also id.*, FIG. 1 (shown at right). Again, this is nothing new as many pre-installed security software programs, such as McAfee, enabled this feature. After registration, the electronic device and ESTSM server are configured to communicate with each other. EX1001, 1:36-2:15.

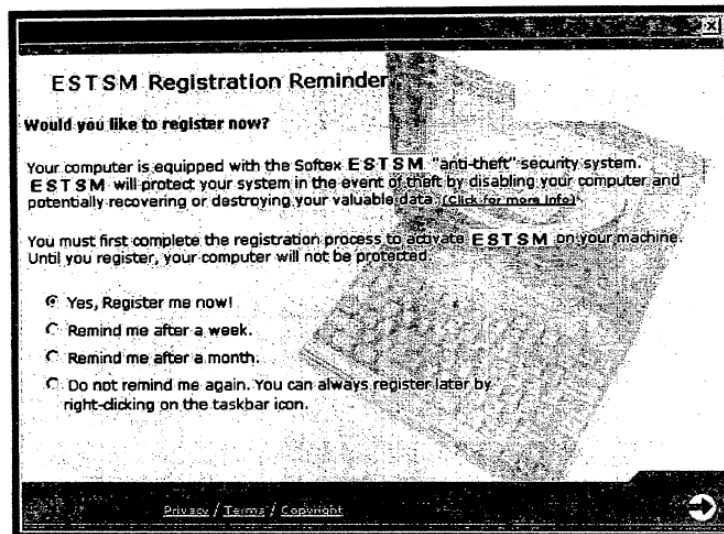


FIGURE 1

“[I]f the device is reported stolen, the ESTSM server may inform the [electronic] device via a secure communications channel to take the appropriate action based on the service options selected by the user (e.g. disabling the electronic device, destroying the storage device (e.g. hard disk drive (HDD)) data, recovering data, encrypting data and more).” *Id.* This was a common response in the pre-2003 era for protecting data on

stolen mobile devices (*see my technology overview above*).

39. Figure 45 of the '649 patent, shown below, illustrates an exemplary ESTSM architecture covered by the Challenged Claims.

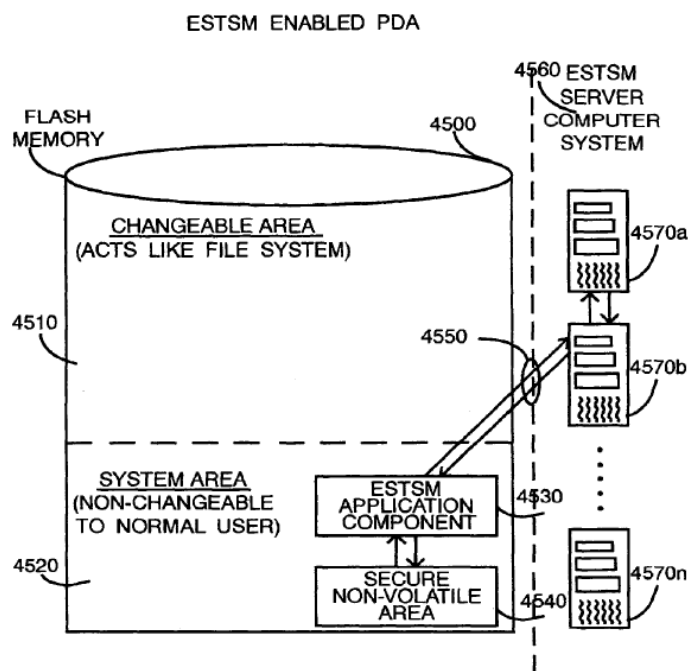


FIGURE 45

As shown, the ESTSM architecture includes “a Flash memory 4500 containing a changeable area 4510 and a system area 4520.” EX1001, 19:8-26. “The system area 4520 may include application components 4530 containing ESTSM application programs” that perform the functions just described. *Id.* The specification explains that “[i]n one embodiment of the invention, the system area 4520 may be non-viewable and implemented in non-volatile memory.” *Id.* This type of memory

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

configuration was well known in the art by August 2003, as discussed above in my technology overview. Memories were known to be separated or partitioned in all sorts of ways and had various levels of security that allowed programs in those separated or partitioned areas to be protected from a normal user.

40. For these reasons, and the specific reasons I discuss below, the Challenged Claims of the '649 patent do not present any novel or inventive features.

VI. APPLICATION OF THE PRIOR ART TO THE CHALLENGED CLAIMS

41. I have reviewed and analyzed the prior art references and materials listed in Part I.B above and discussed in more detail in Part VI.A below. In my opinion claims 1, 7, 9 and 15 of the '649 patent are obvious based on the following prior art, organized into two "Grounds" as set forth below.

Ground	Claim	Basis for Challenge
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

42. I understand that each of the references cited in the grounds above qualifies as prior art to the challenged claims because each reference was filed and/or published before the '649 patent critical date.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

A. Brief Summary of Prior Art

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

43. **Authentication:** zTrace is a collection of webpages from zTrace.com.

I have reviewed these webpages and am familiar with their content. The webpages were captured by Internet Archive and have 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]. I understand that Petitioners have obtained several affidavits from Internet Archive attesting to the accuracy and authentication of these websites and the dates they were publicly available. EX1033 [first archive.org affidavit]; EX1058 [second archive.org affidavit]. I also understand that Petitioners have obtained an affidavit from Dr. Mary Bolin, a librarian and professor with over thirty years of experience with cataloging, researching, and authenticating printed documents, to further authenticate these websites and the dates they were publicly available (as well as authenticating other textbooks and documents used as evidence in this declaration). EX1034 [Bolin declaration]. I understand from counsel that the Patent Office considers these types of affidavits as compelling evidence sufficient to authenticate the accuracy and public availability of webpages. Therefore, for purposes of this declaration, I assume that the zTrace webpages are authentic and qualify as prior art.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

44. With respect to **Exhibits 1026, 1027 and 1028** specifically, I understand that these exhibits have Internet Archive (or archive.org) capture dates that *post-date* the supposed August 23, 2003 priority date of the '649 patent but the content of these exhibits / webpages were actually available *prior to* this priority date. The Petition includes a detailed explanation of how these particular exhibits have been authenticated and why they are prior art. That explanation is reproduced below. I provide additional commentary where needed.

45. **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 [archive.org affidavit], 54.



zControl Released

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

46. **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 same January 15, 2003 date, confirming that this press release

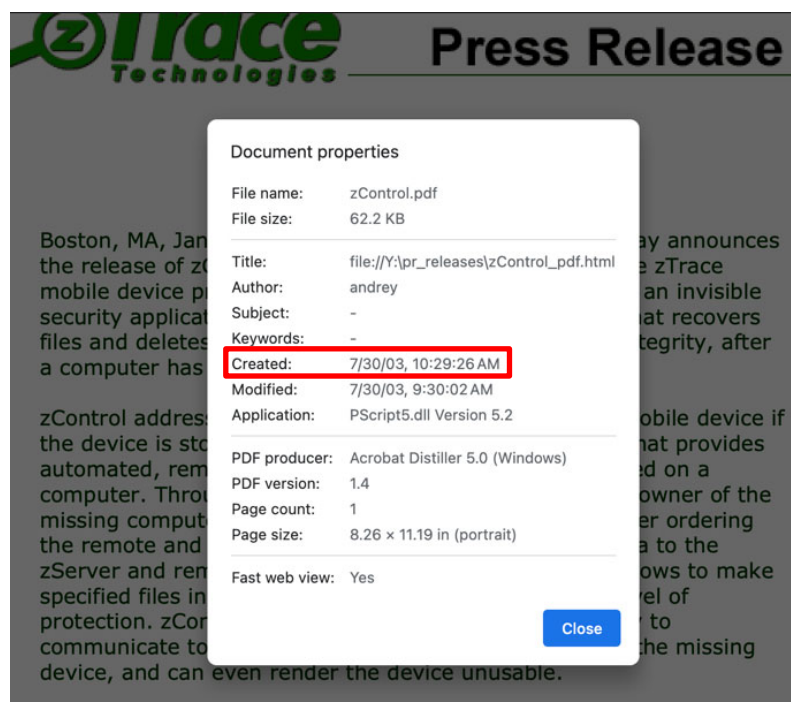
Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

[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

47. Dr. Bolin's affidavit also shows that the html document properties for the press release [EX1026] identify an online creation date of July 30, 2003, which is also before August 23, 2003. EX1034, 83 [Attachment RA] (excerpted, annotated and shown below).



Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

These affidavits therefore indicate to a POSITA that the press release and its content would have been available *before* August 23, 2003 and is therefore prior art.

48. Based on my own assessment of the pre-August 23, 2003 exhibits, there is further evidence that the content of this press release was generally available to the public as early as August 14, 2002. For example, the August 14, 2002 capture of the zControl webpage titled “How Does It Work?” [EX1013] explains that “[t]he ZCONTROL web based user interface enables personal control of the computer’s data even AFTER theft or loss.” EX1013. A POSITA would have understood that at least some of the features described in the zControl press release were already available via this “ZCONTROL web based user interface” prior to the press release, including those related to “retrieving files” and “deleting sensitive information.” EX1013; *compare to* EX1026. Additionally, most of the content in the press release was included in an August 11, 2003 capture of the zTrace.com webpage for the zControl product [EX1053], a portion of which is excerpted below:

How Does It Work?

ZCONTROL is an invisible software application that enables control of the computer's data even AFTER the computer was lost or stolen.

ZCONTROL protects critical and confidential information stored on the computer. The owner of a computer running ZCONTROL can remotely delete or encrypt sensitive files on the computer AFTER the computer is stolen.

ZCONTROL also allows the owner to recover the files from the stolen computer by uploading them to the zTrace server as well as render the whole computer useless by locking its keyboard and mouse, while displaying a pre-defined message to the thief or the person in possession of the stolen computer.

49. EX1028 is a press release for a Yale University collaboration dated

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

August 20, 2003 (excerpted, annotation and shown below) but it has an archive.org
capture date of May 31, 2004. EX1033, 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

50. **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

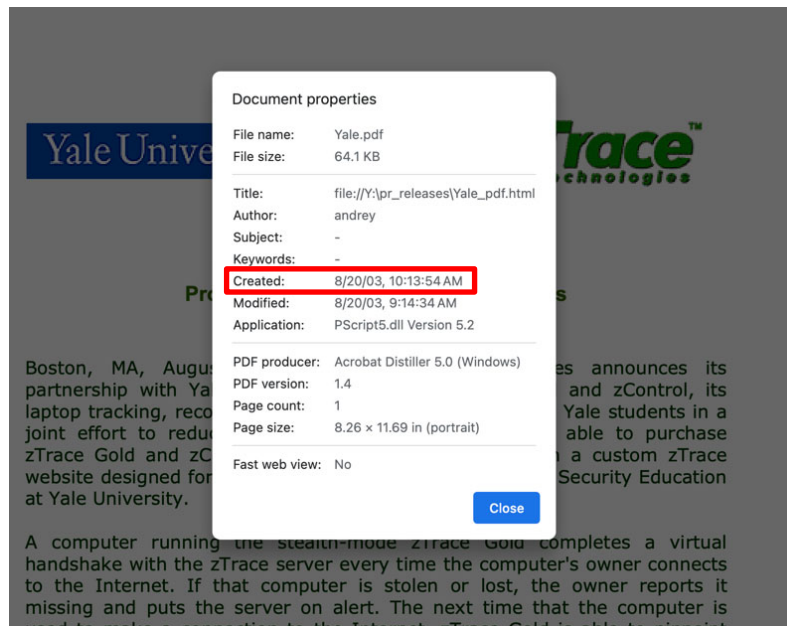


Yale University Selects zTrace to Provide Laptop Protection to Students
Boston, MA, **August 20, 2003**

51. Dr. Bolin confirms that the html document properties for the press
release **[EX1028]** identified an online creation date of August 20, 2003, which is
consistent with the listed date on the press release and is also three days before

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

August 23, 2003. EX1034, 89 [Attachment TA] (excerpted, annotated and shown below).



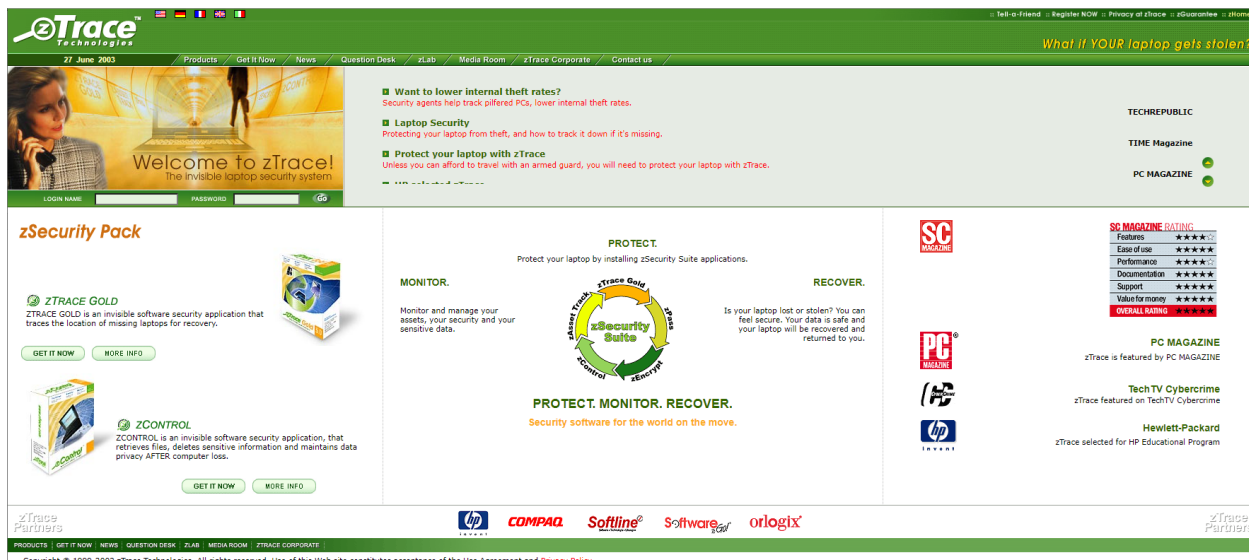
The Internet Archive and Dr. Bolin affidavits therefore indicate to a POSITA that the press release and its content would have been available *before* August 23, 2003 and is therefore prior art.

52. I have reviewed this press release [EX1028] and further confirm that its contents are similar to that of the zControl press release [EX1026] and therefore a POSITA would have understood the details from the press release [EX1028] were publicly available at least as early as the earliest public availability of the zControl press release [EX1026].

53. Furthermore, I am familiar with the zTrace technology and was aware

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

of its commercial presence before August 2003. It was a known company within the technology space. Below is a screenshot of the zTrace.com home page captured by Internet Archive on June 27, 2003 [EX1052], which highlights some of zTrace's achievements:



As shown, zTrace was partnering with the likes of HP and Compaq. EX1052; *see also* EX1024 (announcing zTrace's partnership with HP to supply "HP's customers at K-12 schools, colleges and universities across the country" with security applications). SC Magazine – a reputable online cyber-security magazine — gave them an overall 5-star rating. EX1052. And PC Magazine – another prominent online tech magazine – featured the zTrace technology, as did Time Magazine. *Id.*; *see also* EX1054, 2 (a USA Today article naming zTrace as one of three companies that

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

provide “LoJacks” type security for mobile devices). These are impressive accolades.

54. As mentioned, the home page for the company was zTrace.com. It was publicly available on the world wide web prior to August 2003 without restriction. (See, for example, Yahoo.com’s URL Guide from July 2002 [EX1055], which explains that it “indexed all the Web sites we mention in this issue (Volume 8, Number 7) in section-by-section, page-by-page order” and then identifies “zTrace Technologies” as one of the sites it reviewed. EX1055, 1, 7.) A simple Google search for “zTrace” takes you right to the home page. Even when I entered a date restriction into Google (“before Aug. 23, 2003”) and searched, an April 1, 2002 version of the home page was the first listed search result. An interested party before August 2003 would have undoubtedly known how to navigate to that page and any of its associated sub-pages with the below subject matter with minimal reasonable diligence. I understand from counsel that zTrace had a sizable customer base by August 2003 and, because of its growing popularity, Absolute Software Corp. acquired rights to zTrace’s customer base in March 2005.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

55. **Description:** As previously indicated, the webpages describe a publicly available 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 [Suite page]. Laptop owners download protective software



applications from the zTrace suite onto their laptops via a zServer. EX1019 [FAQ], 2-3; *see* EX1004 (excerpted above). One software application within the zTrace software suite is called “ZTRACE GOLD” – it is “an invisible software security application that traces the location of missing laptops for recovery.” EX1007 [Gold Brochure]. Another is called “ZCONTROL” – it is also “an invisible software application” but it “provides automated control of a computer’s data even AFTER loss has occurred.” EX1013 [zControl How]. Other software applications within the suite include “ZASSET TRACK,” “PASS” and “ZENCRYPT.” EX1005.

56. In use, the zTrace Gold application is installed on the laptop’s hard

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

drive and activates when the laptop connects to the Internet. EX1007 [Gold



Brochure] (shown at left). With each 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.*

57. The registered owner of the laptop can then utilize the zControl application installed on the laptop to protect and recover sensitive information stored on the laptop while the recovery process is underway. For example, 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 [zControl PR]; EX1053; EX1013 [zControl How]. zTrace touts that “[t]here are no icons, files, directories, sounds or ANYTHING visible on the computer, providing total invisibility to the user.” EX1005 [Suite page] (excerpted and shown below).

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

58. I rely on zTrace as the primary reference because it discloses or

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

suggests each of the limitations in the Challenged Claims. As will be discussed, the other prior art that I rely on is merely used to supplement the already suggested disclosures in zTrace. They do not add anything “new” to zTrace. Therefore, in my opinion, zTrace provides one example of a commercially available product before August 23, 2003 that performs all of the functionality that Patent Owner attempts to claim in the Challenged Claims.

59. I understand that the disclosures in zTrace must be enabled for it to be considered a publication for purposes of 35 U.S.C. §§ 102 and 103. In my opinion, the cumulative disclosures in the zTrace webpages provide more than enough details to enable a POSITA to make and use the invention. As indicated above and as will be demonstrated throughout, zTrace describes software applications that perform well known functions that a POSITA could implement with ease and without undue experimentation.

2. Kesler [EX1029]

60. I understand that Kesler is prior art under 35 U.S.C. § 102(b) because it published on April 18, 2002. I also understand that the sole inventor of this publication—Alexander Kesler—is also the creator of the zTrace™ technology described in the webpages above. Kesler, (76); EX1005 [Suite webpage].

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

61. I have reviewed Kesler and have determined that at least some of its disclosures are closely related to the zTrace™ technology described in the webpages above. In particular, Kesler appears to describe some of the same functionality that is performed by the zTrace Gold application in the commercially available zTrace™ product.

62. 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”). But, for the most part, Kesler describes a similar 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 begins with the mobile device owner installing tracing software 12 on the hard drive of her mobile device and then using a registration web page to register 13 the mobile device with the tracking service. Kesler, [0015], [0024]-[0025].

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

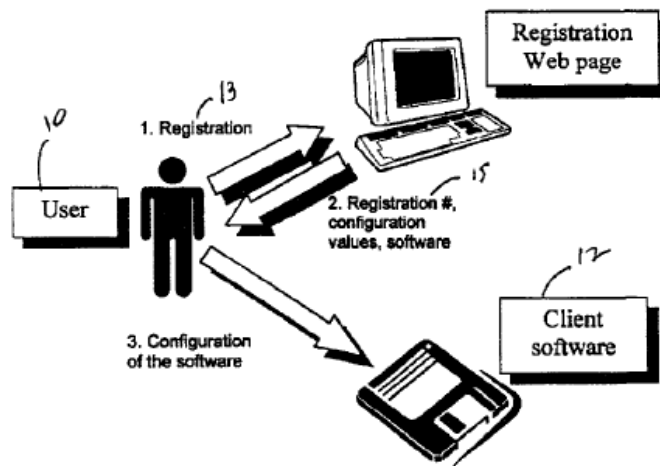
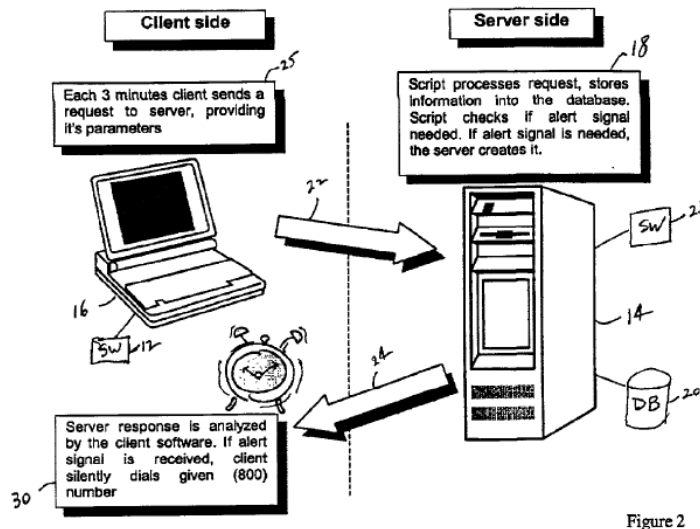


Figure 1

“[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].

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2



63. Kesler provides additional disclosures not found in the zTrace webpages. For example, Kesler discloses that part of its tracing software is “installed onto track zero” of the hard drive. Kesler, [0017]. A POSITA would have known that this is a hidden track like the claimed “**system area**” of the Challenged Claims. 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].

64. Kesler is without a doubt an important complementary reference that can be used to supplement the disclosures of zTrace. Because of the similarities of the disclosures and Kesler’s express mention of the zTrace technology, a POSITA

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

would have looked to Kesler as an informative reference about the zTrace™ functionality. For the same reasons, to the extent Kesler provides details about features that are not elaborated on in the zTrace webpages, a POSITA would have been motivated to look to Kesler to fill the gaps. I understand that one concept for motivation to combine two references is that it would have been “obvious to try” the proposed combination. Here, any disclosures in Kesler would have indeed been obvious to try in combination with the zTrace technology described in the webpages and there would have been a reasonable expectation of success because the disclosures and functionality are so closely aligned in the two references.

3. Isikoff [EX1030]

65. I understand that Isikoff is prior art under 35 U.S.C. § 102(b) because it published on May 5, 1998. I rely on Isikoff to disclose certain “disabling” functionality recited in the Challenged Claims. To be clear, zTrace also discloses disabling and copying functionality but Isikoff provides additional details. Also, to the extent the Board somehow determines that the zTrace press releases are not prior art, Isikoff provides disclosures similar to what is described in the zTrace press releases and can be relied on to effectively replace the zTrace press release disclosures.

66. 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

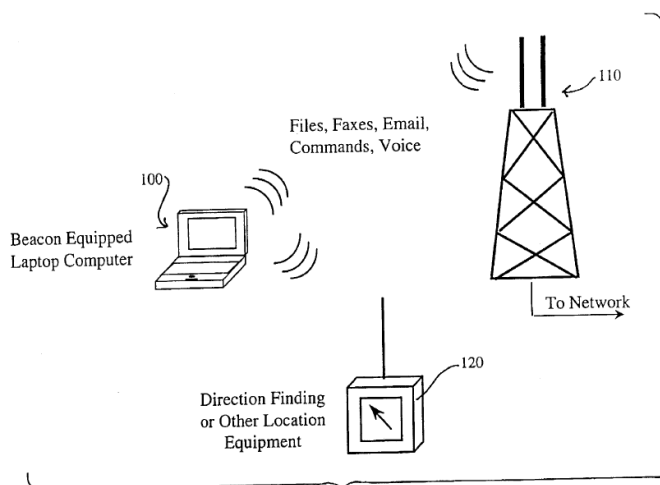
(shown at right). The laptop in

Isikoff includes a beacon

capable of receiving “low-level

control codes” that effectively

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 the

erasure of the hard drive.” Isikoff, 5:59-6:5; *see id.*, Abstract (“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.”), 3:46-53 (“If the computer is stolen the beacon... operates to... disable the

computer.”), 4:3-14 (“various power or device control signals may be routed through

or from the beacon, such that it disables parts of the laptop when the device is stolen,

for example by erasing the hard disc, removing the drive power, or otherwise”),

6:17-30.

4. Bonnett [EX1031]

67. I understand that Bonnett is prior art under 35 U.S.C. § 102(a) because it published on March 13, 2003. Bonnett is relied on to disclose the “**non-volatile memory**” limitations of independent claims 1 and 9 under Ground 1. In particular, Bonnett provides express disclosures of a non-volatile memory with a “**changeable area**” and a “**system area.**” Again, these are features that are suggested by zTrace so Bonnett is simply relied on to fill the gaps and provide more details about this obvious feature.

68. Bonnett discloses a method for securing software programs in memory so that users cannot “delet[e] or corrupt[]” the programs. Bonnett, [0011]. 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 is used to store, for example, “media files [and] data files.” Bonnett, [0036]. The hidden partition is “substantially free from access by a user.” Bonnett, [0032], [0037]. This is where the program is stored. *Id.*

69. The memory in Bonnett can be “a NAND flash memory, or any other suitable volatile or nonvolatile storage and retrieval device or combination of

devices.” Bonnett, [0031]. A POSITA would have known that a “hard drive” is a type of “nonvolatile storage and retrieval device” so Bonnett’s partition disclosures would apply to and could be implemented in a hard drive (such as the one in zTrace).

5. Eckardt [EX1032]

70. I understand that Eckardt is prior art under 35 U.S.C. § 102(a) because it published on April 1, 2003. I rely on Eckardt to disclose the “**non-volatile memory**” limitations of independent claims 1 and 9 under Ground 2.

71. Eckardt explains what was known in the art at the time of the ’649 patent – that “hard disks, including a hard disk on a personal computer, are often ‘partitioned’ into multiple logical subdivisions.” Eckardt, 1:10-16. “Each partition is essentially a separate portion of the disk, which is addressed and handled separately from the other partitions.” *Id.* According to Eckardt, it was known that a partition could be “hidden” such that the partition and its contents “cannot be read or modified.” Eckardt, 1:35-46, 4:50-59.

72. Eckardt’s disclosures are specifically directed to partitioning hard drives so it is directly applicable to zTrace. Eckardt is also assigned to Intel Corp., which is significant, because zTrace discloses that at least its processor is from Intel. This provides motivation to combine Eckardt with zTrace, as a POSITA would know

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

that the technologies in these references would be compatible with each other, and there would be a reasonable expectation of success in combining these references.

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

73. I have reviewed the Petition and agree with the arguments therein. My opinion below are intended to supplement the arguments in the Petition. There may be instances where the language here mirrors the language in the Petition but that is of no matter – my opinions here are my own.

1. Independent claim 1

(a) Limitation 1[a]: “a processor”

74. In my opinion, zTrace discloses this limitation. zTrace is described as “run[ning] on Desktop and Laptop Computers with Windows XP, 2000, ME, 98[,] 386 DX or higher, 16 MB RAM, 2M HD space.” EX1019 [FAQ], 2. The “386 DX” is a known processor produced by Intel. EX1035 [386 DX Textbook], 1 (“386™ DX Programmer’s Reference Manual”). I am very familiar with this processor.

75. Even without this specific disclosure, it was well known at the time of the ’649 patent that Windows-based operating systems were executed by a processor so the laptop running zTrace and the listed operating systems would require a processor. *See, e.g.*, EX1040 [Grandy], 12:1-42 (explaining that “[a] processor unit

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

runs the Microsoft® Windows® XP operating system and performs standard operating system functions[;]” also identifying “Windows® 2000,” “Windows 98” and “Windows® ME” as running on a processor); EX1038 [Windows XP unleashed], 12, 25 (listing hardware requirements for Windows XP, including a “minimum” “CPU Speed” of “233MHz”), 549.

(b) Limitation 1[b]: “one or more non-transitory machine-readable storage media responsive to the processor; and”

76. In my opinion, zTrace discloses this limitation. Again, 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 [FAQ], 2. A POSITA would understand “HD” here to refer to a “hard drive” and “2M” to refer to 2 megabytes. Together, the underlined “2M HD” refers to the program requiring 2 megabytes of hard drive storage space. Hard drives are known “**non-transitory machine-readable storage media**” and therefore the 2M HD hard drive requirement in zTrace satisfies this claim element. This is further confirmed by the ’649 patent, which states that “[s]torage devices such as memory, disk drives, etc. may also be referred to as non-transitory machine-readable storage media.” EX1001, 35:40-42. A “disk drive” is also known as a hard drive (or “HD”). It goes by many names that are used

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

interchangeably – disk drive, hard disk drive, hard drive, etc. *See, e.g.*, EX1001, FIG. 44 (identifying a “hard disk drive”), 2:7 (“hard disk drive (HDD)”), etc.

77. A POSITA would know that a hard drive is “**responsive to the processor,**” as the hard drive typically stores data utilized by the processor. This is basic computer functionality. It is an elementary concept in the computer arts. Hard drives are controlled by software typically including a device driver that commands the hard drive to store or retrieve information on behalf of other software. For example, with respect to the specific processor requirement in the zTrace laptops, the 386™ DX Programmer’s Reference Manual explains that its processor uses the well-known technique of “paging” as a form of memory management that involves storing and retrieving data from the available 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 to 2-2 (“Paging is a mechanism to support a model of a large address space in RAM using a small amount of RAM and some disk storage;” “[T]he operating system uses its paging algorithm to decide which memory pages should be sent to disk.”), 5-1 to 5-2 (“Paging provides access to data structures larger than the available memory space by keeping them partly in memory and partly on disk;” “It allows the operating system to read the page from

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

disk.”), 5-10 to 5-11 (“a program requested reading a sector of disk into memory”), 5-17 to 5-18 (describing pulling and sending page tables from disk storage), 5-21 to 5-22 (“The operating system copies the page from disk storage into physical memory.”), 6-6 (describing the use of device drivers to service disk drives), 6-22 (describing “read[ing] data from a disk file into a buffer”), 9-3 (describing loading a segment from a hard disk), 10-5 (“Paging can be enabled for allowing access to large data structures which are partly in memory and partly on disk.”).

78. In the instance of zTrace, where the zTrace Gold application is in the hard drive (*see* the next limitation), a POSITA would know from the disclosures above that the 386 DX processor in the zTrace laptop would “page” the hard drive to retrieve the code for the zTrace Gold application and then the processor would execute that code when needed to fulfill the zTrace™ services. This same process would be performed for any of the other zTrace applications in the hard drive as well. As I previously mentioned, I am familiar with and have personal knowledge of the innerworkings of the 386 DX processor from Intel and can confirm from my experiences that this is how the processor and hard drive would work to execute the zTrace programs.

79. In sum, because the laptop in zTrace includes the 386 DX processor, it is understood that the processor would use this well-known paging technique to

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

retrieve data from the laptop's hard drive, resulting in the hard drive being
“responsive to the processor.”

(c) Limitation 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:”

80. I understand from counsel that the term “a” is typically interpreted to mean “one or more” absent a clear disclaimer in the specification or prosecution history. I understand from counsel that there are no such disclaimers in the specification or the prosecution history. Based on my review of the '649 patent, there are numerous instances where the ESTSM application is comprised of multiple components or programs and nothing affirmatively limits the ESTSM application to just one application, component or program. *See, e.g.*, EX1001, 2:53-57 (identifying “ESTSM application components”), 3:6-8 (same), 3:32-38 (same), 17:11-13 (explaining that “the ESTSM application components may not be removed from the hard disk drive”), 17:21-28, 17:39-61 (“the ESTSM architecture consists of application components 4405... stored on a hard disk drive[.]”), 19:13-16 (“The system area 4520 may include application components 4530 containing ESTSM application programs”), 23:4-5 (“a system area 4520 for storing ESTSM application components 4530”), 26:11-17 (“the ESTSM application component consists of two

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

sets of programs”), 26:57-27:6 (“the ESTSM application program will cooperate with the other application components to take the appropriate action (i.e. disable the system, erase the hard disk drive, etc”). Thus, consistent with these understandings and my read of the ’649 patent specification, the plain and ordinary meaning of “**a security application**” is one or more security applications.

81. As discussed in the prior art summaries above, 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 applications form the one or more security applications recited in this limitation, as properly construed based on the term’s plain and ordinary meaning.

82. As far as “**the security application [being] operable to perform operations**” recited in the next limitations, the zTrace Gold and zControl applications collectively perform the recited operations. zTrace explains that 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. EX1005 [zSecurity Suite].

83. zTrace discloses that “ZTRACE GOLD is installed on the laptop’s hard drive.” EX1007 [Gold Brochure]; EX1006 [Gold page]. This means that the zTrace Gold application is stored there for use by the processor. Therefore, at least this

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

“security application” is “in at least one of the non-transitory machine-readable storage media.”

84. zTrace appears silent with respect to where in the laptop the zControl application is installed. Although a computer may have multiple types of storage, zTrace only identifies two storage media capable of storing this application – a RAM and a hard drive. *See* EX1019 [FAQ], 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.”). RAM is a short-term memory solution because it is volatile – i.e., it loses all the data stored therein when it is powered off – so this is not an ideal location to install the zControl application if the laptop wants to keep it past the laptop’s first power down event. *See* EX1001, 22:16-18 (“the contents of the main memory 4906 typically are ‘volatile’ and thus are lost when the computer shuts down”), 20:55-64 (identifying “main memory 4906” as a RAM). The hard drive, however, provides a long-term storage solution for the application. As will be discussed for limitation 1[d], a hard drive is non-volatile memory, which means it continues to store data after the laptop is turned off. *See* EX1037, 8 (defining “non-volatile” as “[m]emory which is not lost (i.e. that does not ‘forget’) when the power is shut off.”); EX1001, 22:13-16 (“a ‘nonvolatile’ memory device... means that the memory contents remain intact even when the computer [] powers down”). Storing the zControl

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

application on the hard drive would allow the application to remain on the laptop for as long as needed, or until the application is erased from the hard drive.

85. There are many advantages for including the zControl application on the hard drive. First, as just discussed, the hard drive provides persistent storage for the application so the owner only needs to download the application once and it remains on the hard drive until it is uninstalled or erased, which can be any amount of time needed to further the zTrace™ service. Second, installing the zControl application on the hard drive with the zTrace Gold application would be convenient and would allow these applications to remain “hidden” together in a common location.

86. To this second point, zTrace touts the zTrace Gold and zControl applications as “invisible software security application[s].” EX1007 [Gold Brochure]; EX1013 [zControl How]. I discuss the “invisible” nature of these applications with respect to limitations 1[e] and 1[f] but, for purposes of this limitation, a POSITA would have understood this disclosure to mean that the applications reside in secure areas on storage media. The secure area could be, for example, a hidden area on the storage media. Or, as I discussed in my technology overview, the secure area could be an area with a specific security level.

87. Hard drives were known to have secure or hidden areas. For example,

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Kesler discloses that part of the client software is “installed onto track zero” of the computer’s hard drive. Kesler, [0017]. It is well known that track zero is a hidden track. This is what allows Kesler’s software to “download invisibly,” which “significantly reduces the opportunity for tampering.” Kesler, [0017]. Eckardt refers to hidden hard drive partitions as “illegal” partitions and explains that these partitions were not recognized by the operating system and were used to store “programs that the end user must not modify in any way,” similar to what zTrace describes for its applications. Eckardt, 1:10-49. Cotichini similarly identifies a portion of its hard drive as “protected storage” that requires a secure key to access. Cotichini [EX1039], FIG. 20, 29:24-38. Numerous other examples exist. Again, I talk about this in great length with respect to limitations 1[e] and 1[f] and incorporate those opinions here to the extent they are relevant.

88. Thus, in my opinion, because the zTrace Gold application is installed on the laptop’s hard drive, a POSITA would have understood that the zTrace Gold application is in a secure area of the hard drive that keeps the application invisible to normal users of the laptop. To the extent Patent Owner’s argue that zTrace’s disclosures are not clear on this point (they are), a POSITA would have at least found it obvious that this application is installed in a secure area of the hard drive because those secure or “hidden” areas are known to keep the application “invisible” to a

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

normal user of the laptop. zTrace's disclosures provide express motivation to install the zTrace Gold application in that location. Kesler explains that its zTrace-related client software is installed on a hidden track. And these types of partitions were already well known in the art so homing the application in this area on the hard drive would have been well understood both in reasons why to house in that location and how to install at that location, and would have been obvious to try. Again, my opinions from limitations 1[e] and 1[f] again apply and are incorporated by reference.

89. Note that I use the term “normal user” throughout my declaration. By this I mean, a typical person using the computer who does not have any specialized software, keys or “hot keys”, or other advanced technical information that would allow him or her to gain special access to the computer or its components. *See, e.g.*, Eckardt, 1:35-46 (identifying “a system integrator” or “trained personnel” as needing special access to hidden portions of the hard drive for specific purposes). The '649 patent also refers to certain features as being applied to a “normal user.” For example, in Figure 45 of the '649 patent, the figure includes language specifying that the “system area” is “non-changeable to [a] *normal* user.” The '649 patent therefore also recognized the difference between normal users and other users.

90. Turning back to limitation 1[c], a POSITA would have understood that

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

the zControl application is installed onto the hard drive for the reasons discussed above – there are limited storage solutions identified, only the hard drive is ideal for long term storage, and co-locating the applications would have its advantages. A POSITA would have also found it obvious to try installing the application onto the hard drive for these same reasons.

91. A POSITA would have further understood that the zControl application is also in a secure area of the hard drive (or possibly the same secure area as the zTrace Gold application) so it too remains “invisible” to the laptop users. A POSITA would have at least found it obvious that this application is installed in a secure area of the hard drive because those secure or “hidden” areas are known to keep the application “invisible” to a normal user of the laptop. zTrace’s disclosures provide express motivation to install the zControl application in that location. Kesler explains that its zTrace-related client software is installed on a hidden track. Kesler, [0017]. And these types of partitions were already well known in the art so homing the application in this area on the hard drive would have been well understood both in reasons why to house in that location and how to install at that location, and would have been obvious to try. Again, my opinions from limitations 1[e] and 1[f] again apply and are incorporated by reference.

92. Thus, a POSITA would have understood, or at least have found it

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

obvious, that the zControl application is installed on the laptop's hard drive. For at least these reasons, zTrace suggests or renders obvious that this **"security application"** is also **"in at least one of the non-transitory machine-readable storage media."** Thus, zTrace discloses, suggests and/or renders obvious **"a security application in at least one of the non-transitory machine-readable storage media."**

* * *

93. To the extent Patent Owner can demonstrate that **"a security application"** means a single application, it is my opinion that zTrace would still render this limitation obvious. zTrace explains that its applications "[c]ollectively" "provide the optimum wrap around security solution" for its customers. EX1005 [zSecurity Suite]. The "[s]uite 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 integrated 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 [FAQ], 3 (Q: "Can I remove zTrace™?" A: "A subscriber can remove *the program* from his/her computer using a personalized password"). This "program" can be the claimed single **"security application."** Alternatively, these disclosures provide the

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

teaching and suggestion to motivate a POSITA to combine the applications into a single application, as zTrace already viewed its solutions as a single program or application.

94. With respect to the zTrace Gold and zControl applications specifically, zTrace created a “zSecurity Pack” in early 2003 that included only these two applications. EX1026 [zControl PR]; EX1052. 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. Because of the complementary nature of these applications, a POSITA would have found it obvious to combine at least these two applications into a single application or program that satisfies the single “**security application**” requirement (should Patent Owner successfully demonstrate that this term should be construed differently from its plain and ordinary meaning). The applications are already manufactured and sold as a single product / package and combining them into a single application or program would have been a straight-forward and elementary

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

task for a programmer that would have had every reasonable expectation of success.

95. As will be discussed in more detail throughout, the computer arts are highly predictable, and the trivial modifications proposed in this declaration would not have posed a technical obstacle for even the most junior programmer and would have had every reasonable expectation of success. There is nothing about these applications that would suggest that they would be challenging to combine. For example nothing about these applications requires special resources or would have aspects that would make adding features problematic.

96. 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. These applications were already understood to co-exist in the hard drive together (or at least it would have been obvious for them to co-exist in the hard drive together) so, as mentioned, it would have been a relatively elementary task for a programmer to combine them into a single application.

97. Kesler provides further motivation and evidence that it would have been obvious to combine the applications into a single application and increases the reasonable expectation of success. 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. A module is a block of code dedicated to a specific function. It extends the functionality of the main program. They were well known in the art at the time of the '649 patent.

98. For example, Kesler points to Figure 3 (shown below) and explains that “the client tracing software 32 includes three main modules: zAgent 34, zCore 36, and zTrace 38.” Kesler, [0035].

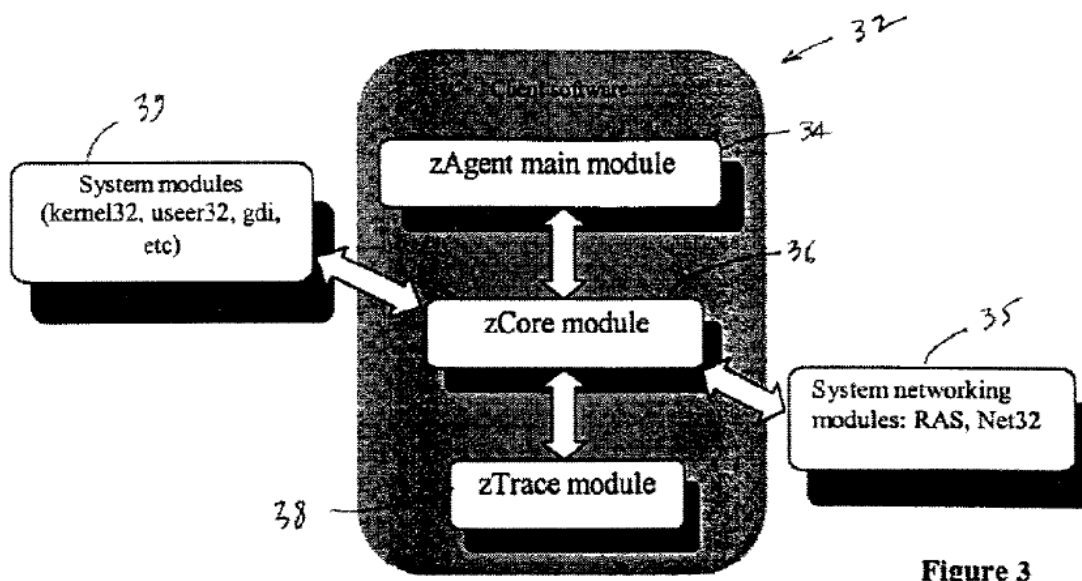


Figure 3

According to Kesler, “[t]his architecture allows the zTrace software to use system resources effectively and to be easily extended in the future.” Kesler, [0035]. In other words, Kesler contemplated adding more modules (or blocks of code for performing

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

specific functionality) to the zTrace software in the future that would expand the functionality of the main program. But, as illustrated in Figure 3 and as would be understood by a POSITA, the modules are part of the main program 32 and are thus part of a single application.

99. A POSITA would have understood or at least found it obvious that the zTrace Gold and zControl applications (and/or any other application in the zTrace™ suite) could be designed in a similar manner to the program in Kesler such that they are *modules* and extensions of a main program. As explained in Kesler, this architecture advantageously allows for flexibility to add functionality. Kesler, [0035]. Kesler's disclosures are particularly compelling because the relevant embodiment discussed here explicitly identifies a zTrace module that performs the same or similar functionality as the zTrace Gold application of the zTrace™ service. *Compare* Kesler, [0037] ("zTrace controls [the] phone calling process, gathering of the identifying information and tracing of the computer's location."), *with* EX1007 [Gold Brochure] ("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.... It recognizes and traces through both internal and external networks for LAN/WAN configurations to pinpoint [the] actual location of the missing laptop."). Kesler's sole inventor is also

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

the creator of the zTrace™ product and service so a POSITA would have been extremely motivated to look to Kesler's disclosures for details about the zTrace™ technology or potential features / functionality that could be added to the commercially available zTrace™ technology with a reasonable expectation of success.

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

(d) Limitation 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;”

101. In my opinion, this limitation is disclosed and/or rendered obvious by zTrace. The notion of registering a device for a particular service was nothing new in August 2003. Indeed, anyone who owned a computer at that time can recall launching his/her computer operating system for the first time and being forced to register the computer with the operating system provider (e.g., Microsoft) and then going through the process of installing and registering certain drivers on the computer so that peripheral devices were compatible with the system. This routine registration is documented in U.S. Patent No. 6,775,828 to Feinleib et al. [EX1041],

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

which is assigned to Microsoft. *See* EX1041, 1:10-56. Security software, like McAfee's anti-virus software, which was popular at the time, also required registration and installation to commence protection services on the computer. *See* EX1042, (73), 3:44-65; *see also* EX1043, 67:26-44.

102. zTrace generally explains that owners must register their laptops with the zServer prior to receiving laptop protection services. For example, 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 [Overview], 1 (“Welcome to zTrace!... Register Now!”). 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 [FAQ], 2; *see also id.*, 3 (“you can unsubscribe from zTrace™ by uninstalling zTrace™ from your computer;” “The new owner of your computer will have to subscribe for the service to get zTrace™”). The FAQ page also states that “[t]he information you entered during registration” is “used to notify you when your computer is found.” *Id.*, 2.

103. zTrace also makes clear that the laptop itself is registered. For example, zTrace explains that when the owner purchases a new laptop, “just resubmit your registration, and your new computer will be zTrace™ protected too.” EX1019

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

[FAQ], 3. “[Y]ou can simply cancel your subscription with [the old] computer.” *Id.* The registration is therefore on a per-device basis. *See also* EX1007 (where the specific zTrace Gold application on the laptop is further “registered with the zSERVER with a unique identification”). Thus, zTrace discloses that “**an owner of the mobile electronic**” “**register[s] the mobile electronic device with a security service.**”

104. zTrace discloses that its “**security service resid[es] at least partially on one or more servers.**” For example, 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 [Gold Brochure], 1 (“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.

105. 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. zTrace explains that “ZTRACE GOLD is installed on the laptop’s hard drive and registered with the zSERVER with a unique identification.” EX1007 [Gold Brochure]. This sequence indicates that the application is first installed and

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

then registered with the zTrace™ service. This is further confirmed by disclosures in Kesler, which disclose that “the client part 12 is installed by the user on his computer 16” and “[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].

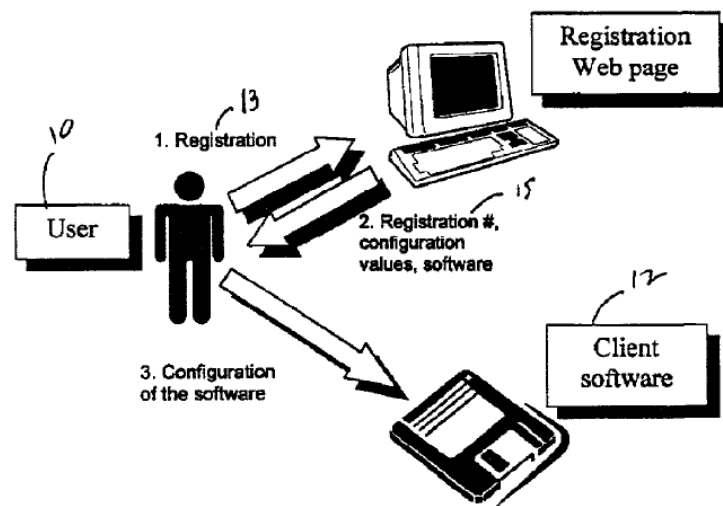


Figure 1

This is further illustrated in Figure 1 of Kesler, shown above, where the “registration #” and certain “configuration values” are sent via the registration webpage to the laptop for “configuration of the software.” As I previously mentioned, the functionality described in Kesler overlaps substantially with the zTrace Gold application so Kesler evidences that at least the zTrace Gold application would perform similar install and register functionality. In other words, installing the applications onto the laptop *enables* the owner to register the laptop with zTrace™

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

services, and zTrace would need to be installed on a laptop prior to registration in order for zTrace to assign a unique identifier to the laptop.

106. Furthermore, it is my opinion that zTrace's disclosures suggest 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 [FAQ], 2. As previously discussed, these wizards were known in the art well before August 2003. In the Feinleib patent, the specification explains that "the software is first installed" and the "[r]egistration wizard 118 collects this registration information by prompting the user for inputs." EX1041, 3:66-4:10. This information is then transmitted to a remote server for storage. *Id.*, 1:38-56. This is how a POSITA would have understood the wizard in zTrace to work as well. 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. *See also* Kesler, [0033]-[0034] (describing how the system updates installed version of the software).

107. This is further evidenced by zTrace's unsubscribe process. zTrace states that "you can unsubscribe from zTrace™ by uninstalling zTrace™ from your

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

computer.” EX1019 [FAQ], 3. In my opinion, 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.

(e) Limitation 1[c][ii]: “causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;”

108. In my opinion, this limitation is disclosed by the combination of zTrace and Kesler. As will be demonstrated herein, zTrace suggests the functionality recited in this limitation and Kesler provides the details to render this limitation obvious.

109. The zTrace Gold Brochure, which forms part of the zTrace reference, 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 [Gold Brochure]. 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 indeed correlated.

110. Kesler discloses that “[a]fter registering 13, the user is automatically

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

assigned a registration number 15 that uniquely identifies the client in a database 20 associated with the tracing server 14.” Kesler, [0024], FIG. 1 (below at right). Kesler explains that this unique

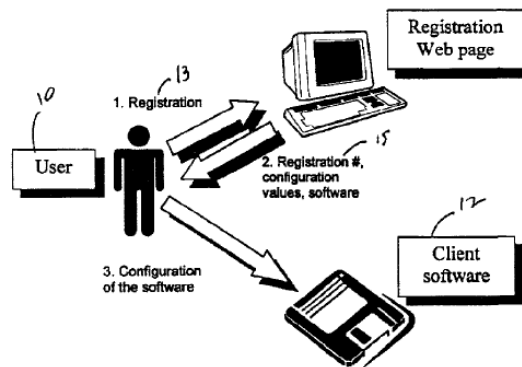


Figure 1

registration number, along with other identifying information, is sent to the tracing server as part of a client report each time the client software connects to the Internet. Kesler, [0025] (“[W]henver the client software determines that the computer is connected to the Internet, the client tracing software sends 22 another report to the

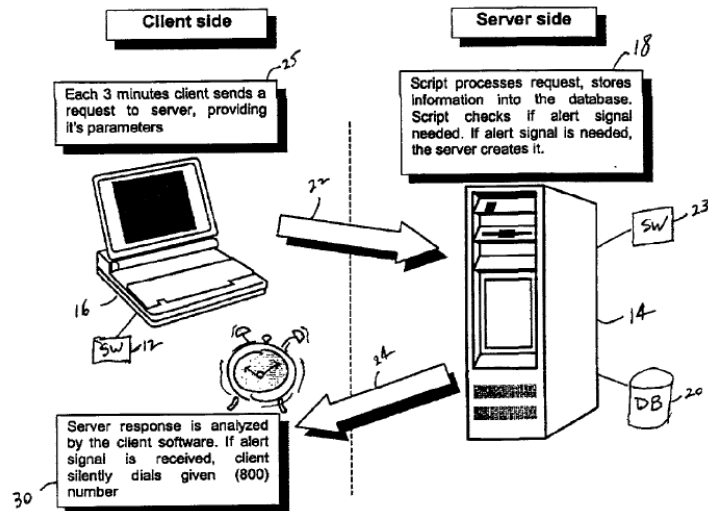


Figure 2

“unique by default.”), FIG. 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] (“The server tracing software 23 analyzes the client information to

tracing server and receives responses 24.”), [0026] (“Each client report includes... the client’s assigned registration number, and the system ID of the computer[,]” which is

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

make sure that the received system ID matches the locally stored system ID and makes a decision whether or not to respond with an alert.”), [0034]-[0035], [0005] (explaining that if “a mobile device communicating with the server is marked in the server’s database as ‘stolen,’ an alert signal is generated towards this communicating client device”).

111. It would have been obvious to a POSITA to combine zTrace with Kesler. This combination would have predictably resulted 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. This combination would have further been obvious to try for at least the reasons discussed below as well as those previously discuss in connection with zTrace and Kesler.

112. A POSITA would have perceived no technological obstacle to the proposed combination, for the reasons set forth below, and would have had every reasonable expectation of success. Modifying zTrace based on the disclosures in Kesler would have been easy and straight-forward to implement as including this identifying information in the zTrace Gold’s check ins with the zServer is a simple matter of sending data to the zServer that the zTrace Gold application already had in

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

its possession (i.e., the assigned registration number) or could have easily acquired (i.e., the system ID). With respect to the system ID, for example, zTrace discloses a zAsset Track application that collects “[s]ystem serial numbers” for the laptop. EX1016 [zAsset Track page]. The zTrace Gold application could obtain the system serial number from this other application and forwarded as part of its check-in as just discussed.

113. A POSITA would have had clear motivations to combine. First, as discussed throughout, Kesler is an analogous reference to zTrace because Kesler’s sole inventor is also the creator of the zTrace™ technology and the references discuss similar technology (*see* prior art summaries above and my relevant opinions throughout). A POSITA would have undoubtedly been motivated to look to Kesler’s disclosures for details about certain functionality of the zTrace™ technology and/or possible enhancements to that technology and would have understood that any combination would have had every reasonable expectation of success.

114. Second, the disclosures in Kesler provide the teaching, suggestion and motivation for this combination and resulting functionality. Kesler expressly identifies zTrace technology in its disclosures. For example, in one embodiment of Kesler, the client software is described as including three modules – zAgent 34, zCore 36, and zTrace 38 – that perform the functionality described above. Kesler,

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

[0035]. “The zAgent realizes basic client functionality.” Kesler, [0036]. “The zCore module implements all communication functionality.” Kesler, [0037]. And, “zTrace controls [the] phone calling process, gathering of the identifying information and tracing of the computer’s location.” *Id.* While these disclosures may not align exactly with what is described in the commercially available zTrace service documentation that forms the “zTrace” reference, they overlap considerably and that would have been enough to motivate a POSITA to combine zTrace with the disclosures of Kesler.

115. As I mentioned for limitation 1[c], the zTrace Gold application includes functionality similar to the “zTrace” module in Kesler. The zTrace Gold application also embodies the “zCore” module functionality from Kesler because the application handles communications to and from the zServer. *See* EX1007 [Gold Brochure]. Again, this overlapping functionality would have provided the teaching, suggestion, and motivation to combine zTrace with Kesler. A POSITA would have therefore been motivated to modify the zTrace Gold application based on the disclosures in Kesler so that the application gathers and sends identifying information to the zServer as part of its communications.

116. Third, 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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

one of the key ways for a transmitting device to identify itself to a receiving device. Isikoff, 9:53-63 (describing a laptop beacon that “transmit[s] its ID”), 9:64-10:10 (“it compares the beacon ID number to the received address... [and] then performs one or more of the... internal security actions”), 10:11-31; Cotichini, 3:54-4:7 (“These first signals contain the encoded identification (serial number) of the sending computer”), 4:15-29 (“The remote station receives the queries and decodes the encoded identification information in order to determine if the client computer matches an entry on a list of reported lost or stolen computers.”), 8:33-51, 16:1-9, 30:34-37. This identification provides a form of authentication that the receiving device can use to ensure that it is communicating with an approved or authorized device.

117. A POSITA would have known that, 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 communicating with the zServer. EX1007 [Gold Brochure]. 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 [Gold Brochure] (“ZTRACE GOLD is an invisible software security

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

application that traces the location of missing laptops for recovery.... When the missing computer connects to the Internet, the stealth application receives a signal from the ZSERVER and the computer reports its own location.... The computer's location and registration information are used by the ZTRACE Recovery Team, who works directly with the police department to recover the missing property.”), EX1006 [Gold page]. This would render zTrace™ services useless.

118. With respect to “**automatically**” sending this information, zTrace discloses that “[e]very time the laptop is connected to the Internet, ZTRACE GOLD checks with the ZSERVER to determine the laptop’s status.” *See* EX1007 [Gold Brochure]. zTrace makes clear that this communication is “stealth” and occurs without any user involvement. *See id.* (“zTRACE GOLD operates in stealth mode, with no directories, files, icons, or sounds ever appearing on the laptop.”); EX1019 [FAQ], 2-3 (“zTrace Gold becomes active only when the computer connects to the Internet[;]” “Can the user hear the modem when zTrace makes a call? No[.]”), 3 (“If the method of Internet connection is changed (e.g., cable modem to dial up) – the software is intelligent and determines the best method to connect to the Internet in a stealth fashion;” “Can zTrace work through firewalls to reach the Internet? Yes – the core technology penetrates the majority of firewalls and proxy servers to automatically [] provide optimum security in a corporate setting.”). This

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

communication and the data sent to the zServer occurs “**automatically.**”

119. Furthermore, my opinions regarding “periodically communicat[ing]” for limitation 1[c][iii], apply here with respect to the automatic functionality of the zTrace Gold application to zServer communications. A POSITA would have known that the identifying information is sent with each communication with the zServer. So, for the same reasons that this periodic communication is automatic, the communication here for limitation 1[c][ii] is automatic.

120. Thus, for these reasons, it would have been obvious for the zTrace Gold application 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. Limitation 1[c][ii] is therefore rendered obvious by the combination of zTrace and Kesler.

- (f) **Limitation 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;”**

121. This limitation is rendered obvious by the combination of zTrace and

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Kesler.

122. 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 [Gold Brochure] ("ZTRACE GOLD is installed on the laptop's hard drive and registered with the ZSERVER with a unique identification"). Then, "[e]very time the laptop is connected to the Internet, ZTRACE GOLD checks with the ZSERVER to determine the laptop's status." EX1007 [Gold Brochure]. Thus, zTrace discloses that **"after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to... communicate with the security service."**

123. Because it is known that no Internet connection and communication is possible when the laptop is turned off, zTrace also discloses 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."** This is consistent with the disclosures in the '649 patent, which indicate that messages are sent "periodically while the system is connected to the Internet." EX1001, 27:3-6; *see also id.*, 26:11-17, 27:31-35, 34:55-63.

124. Although zTrace appears silent with respect to any **"periodic[] communicat[ion]"** with the zServer after the zTrace Gold application's initial

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

check-in with the zServer at the time the Internet connection is first established, it is my opinion that the commercially available zTrace™ service would have included this functionality to be viable and to further its purpose of quickly and efficiently recovering stolen laptops. *See, e.g.,* EX1028 [Yale PR] (“This guarantees students that their lost computer will be recovered in the quickest time possible, which is what zTrace Gold is all about.”). zTrace also boasts that its “applications provide constant protection to mobile devices and the data stored on them” and that its technology “enable[s] and enforce[s]” an “‘always-on’ security policy.” EX1024 [Suite PR]. Regular, periodic communication with the zServer would facilitate this “constant” “always-on” protection.

125. For purposes of this proceeding, however, I rely on Kesler’s express teaching that its client software “**periodically communicat[es]**” with the remote server run by the security service provider. More specifically, 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.”).

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

126. It would have been obvious to combine the Internet-checking timing structure of Kesler with zTrace, predictably resulting in the zTrace Gold application checking for an Internet connection at pre-determined intervals and then communicating with the zServer if it is available. This type of periodic communication was well known in the art by August 2003. Cotichini and Isikoff – two references that disclose similar systems for tracking and recovering mobile devices – disclose the use of periodic communication with a remote server as part of its protocol for determining whether the mobile device has been reported stolen. *See* Cotichini, 3:1-17 (describing “an electronic device with an integral security system” that “includes means for sending signals to a remote station at spaced apart intervals of time. The signals include identifying indicia for the electronic device.”), 11:32-50, 20:60-67, 30:7-11; Isikoff, 9:64-10:10 (discussing “designated message interval[s]”). Implementing this timed interval feature into zTrace would have been trivial. A POSITA would have perceived no technological obstacle to the proposed combination, and would have had every reasonable expectation of success. At the very least, this modification would have been obvious to try in zTrace.

127. zTrace’s disclosures provide the teaching, suggestion and motivation for this modification. As I just mentioned, implementing this functionality would have furthered zTrace’s objective to enable “constant” “always-on” protection.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

EX1024 [Suite PR]; *see also* EX1028 [Yale PR]; EX1020 [zGuarantee page]. For example, connecting at regular intervals allows the zTrace Gold application to more frequently check for any changes in the laptop's status. If, for example, the laptop only connects to the Internet once per day but stays connected for long periods of time (e.g., hours), then the zTrace Gold application could miss that the laptop owner reported the laptop stolen because it was reported *after* the laptop initially connected to the Internet. But, if the laptop continued to communicate with the zServer at pre-defined intervals *while* connected to the Internet, then the zTrace Gold application would receive the report from the zServer at its next interval check in instead of at the next time the laptop connects to the Internet, which could be in hours or days. The application's response time for sending its location and performing any data recovery-related actions triggered by the report (*see* limitations 1[c][v] and 1[c][vi] below) would be measured on the order of minutes, as opposed to hours or days, increasing the effectiveness of the zTrace™ service. Increasing the response time could also result in a faster recovery time for the laptop itself.

128. It is also my opinion that the zTrace™ service would have benefited from the laptop continuing to check in with zServer at this interval even *after* it receives notice of being reported stolen, as it would allow the laptop to regularly provide its location (which would have obvious benefits for zTrace's recovery

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

service if the laptop's location changed), and to check for later-provided instructions from the laptop owner related to copying files, deleting files, or disabling laptop functionality, as will be discussed in more detail in later limitations 1[c][v] and 1[c][vi]. *See, e.g.*, EX1026 [zControl PR] ("Through the zControl web-based interface an owner of the missing computer can communicate with his/her computer ordering the remote and invisible deletion of files, recovery of data to the zServer and remote encryption of data... and can even render the device unusable"); EX1053.

129. A POSITA would have realized other benefits of incorporating timed intervals for checking the Internet into zTrace. For example, Kesler explains that connecting at regular intervals "reduces the need to synchronize the local and server timelines." Kesler, [0033].

130. It further would have been obvious to combine zTrace with Kesler for the reasons previously mentioned in other sections.

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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

- (g) **Limitation 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;”**

132. In my opinion, this limitation is rendered obvious by (1) zTrace alone, (2) zTrace in view of Kesler, or (3) zTrace in view of Isikoff and/or Kesler.

133. 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.”**

134. With respect to **“accepting a notification at the mobile electronic device from 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 [zTrace How]; EX1019 [FAQ], 2 (instructions to the laptop owner for reporting theft); EX1028 [Yale PR]. 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 [Gold

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Brochure]; *see also* EX1028 [Yale PR]. 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].”**

135. A POSITA would have understood this signal 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 only when the laptop is reported missing. *See* EX1007 [Gold Brochure] (“zTRACE GOLD... traces the location of *missing* laptops for recovery;” “*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;” “The computer’s location and registration information are used by the zTRACE Recovery Team... to recover the *missing* property.”); EX1006 [Gold page]; EX1028 [Yale PR] (“zTrace Gold is able to pinpoint the computer’s exact location so that authorities are able to recover and return it”).

136. Kesler confirms the details about the zServer’s messaging. Therefore, to the extent additional details are required to satisfy this claim element, I rely on Kesler in combination with zTrace. Kesler discloses that its “tracing server will

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

communicate with the stolen computer, notifying it that it was stolen.” Kesler, [0017]. Kesler’s claim 10 similarly recites “software capable of configuring a device to receive a message from a server indicating a possibility that the device has been stolen[.]”

137. It would have been obvious to modify zTrace, based on the disclosures of Kesler, so that the zTrace Gold application receives a similar message from the zServer notifying it that the laptop has been reported stolen. This is essentially what zTrace already describes – Kesler merely fills in the details. For this reason alone, combining zTrace with Kesler in this manner would have been obvious to try.

138. As discussed throughout, Kesler provides express teachings, suggestions and motivations to combine with zTrace. *See, e.g.*, my opinions regarding limitations 1[c], 1[c][ii] and 1[c][iii]. Kesler’s sole inventor created the zTrace™ service and Kesler itself includes embodiments that explicitly identify “zTrace” modules. A POSITA would have therefore been motivated to look to Kesler’s teachings for more details about the signal received at the zTrace Gold application from the zServer and further would have found it obvious to try implementing Kesler’s notification/message in zTrace.

139. The combination results in a trivial modification that would have been straight-forward to implement and could be done with a reasonable expectation of

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

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. 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. *See* my opinions regarding limitation 1[c][ii]. A POSITA would have been further motivated to combine Kesler with zTrace for the reasons discussed in previous limitations. *See, e.g.,* my opinions regarding limitations 1[c], 1[c][ii] and 1[c][iii].

140. 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.**”

141. 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.

142. With respect to zTrace alone, as previously discussed, the zControl application “provides automated control of a computer’s data.” EX1013 [zControl How]. “Through the zControl web-based interface an owner of the missing computer

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

can communicate with his/her computer... and can even render the device unusable.” EX1026 [zControl PR]; *see also* EX1053 (zControl... render[s] the whole computer useless by locking its keyboard and mouse”); EX1028 [Yale PR] (“Through zControl, students will be able to remotely... render the computer useless by remotely locking all its functions. zControl is therefore able to remotely control the visibility and access to a student’s files as well as the computer itself.”); EX1013 [zControl How]. 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 appears to communicate with the laptop and the zControl application must receive (or “**accept[]**”) these directives to execute them.

143. A POSITA would have understood that the zServer receives the disable directives from the web based user interface that the owner interacts with and then the zServer sends the directive to the zControl application for execution. Or, at the very least this communication configuration would have been obvious to try because there are only so many ways the zTrace applications can communicate with the zTrace™ service provider and the zServer is the only component within the service provider system that appears to talk with the zTrace applications on the laptop. This modification would have been easy to implement and would have had every

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

reasonable expectation of success. This disable functionality would have therefore been understood to be a message from the zServer. *See, e.g.*, EX1037, 214 (defining “disable” as “prevent[ing] a hardware device from working” and further “refers to a tone or other signal which you send over a phone line to disable the equipment at the other end.”). 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.”**

144. To the extent additional details are required to satisfy this claim element, they are disclosed by Isikoff. For example, 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 (“An object tracking, communication, and management system for a laptop computer or similar device, 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.”), 3:46-53 (“If the computer is stolen the beacon... operates to... disable the computer. The particular security measures to be effected may be set in advance, or may be controlled by an external communication, in which case

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

the user... may make the decision as to which of these steps is appropriate.”), 4:3-14 (“various power or device control signals may be routed through or from the beacon, such that it disables parts of the laptop when the device is stolen, for example by erasing the hard disc, removing the drive power, or otherwise”). Isikoff explains that, when the laptop is reported stolen, the beacon receives “low-level control codes” that effectively 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 the erasure of the hard drive.” Isikoff, 5:59-6:5; *see id.*, 6:17-30 (“The purpose of the low-level codes is to perform the emergency functions under extreme circumstances.”). 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.

145. In my opinion, 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. The remote user at the zControl web-based interface can send directions to disable the laptop to the

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

zServer, which then forwards the directions to the zControl application for execution, as I previously discussed for zTrace alone. 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.

146. zTrace provides teachings, suggestions and motivations for this combination. For example, zTrace explicitly discloses the use of “[p]redefined actions,” which include “retrieving files, [and] deleting sensitive information,” and explains these “[a]ction[s] can be triggered by... a zTRACE loss report.” EX1013 [zControl How]. 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 [zControl How]; EX1005 [zSecurity Suite page]. As previously discussed, later iterations of zControl provided remote access to this disable functionality, which suggests that it was an important feature for protecting data. Adding a disabling feature to predefined actions would have been trivial and there would have been every reasonable expectation of success.

147. zTrace teaches the use of disabling functionality at a high-level. A

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

POSITA would have therefore been motivated to seek more information about how to implement this functionality and would have considered Isikoff because of its exemplary details on remotely disabling mobile devices that have been reported lost or stolen. Isikoff, 1:59-65. As also discussed for previous limitations, Isikoff discloses several other features that are described or are at least beneficial to the zTrace™ service (*see* my opinions regarding limitation 1[c][ii] and 1[c][iii]) so Isikoff in general would have been viewed as an important complementary reference to zTrace.

148. The concept of remotely disabling devices was also well known by August 2003. Indeed, as mentioned before, Netwon's Telecom Dictionary from 2001 includes a definition for "disable" that "refers to a tone or other signal which you send over a phone line to disable the equipment at the other end." EX1037, 214.

149. For these reasons, it would have been obvious to try combining zTrace with Isikoff. Any modifications to zTrace would have been trivial and there would be a reasonable expectation of success.

150. 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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

be the single application that receives both types of messaging from the zServer. This, again, would have been an obvious implementation of the zTrace applications for the reasons I discussed for limitation 1[c], which apply here.

151. Isikoff is analogous art to zTrace and Kesler, as it teaches a similar mobile device protection and tracking system. Isikoff, 1:59-65 (“the beacon is activated with a security control program to secure crucial data in the computer’s storage... [and] is preferably also trackable to locate and recover the stolen computer”); EX1005 [Suite page]; 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.

152. For these reasons, the prior art renders limitation 1[c][vi] obvious.

(h) Limitation 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”

153. As just discussed, zTrace alone or zTrace in view of Kesler renders

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

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 [Gold Brochure]; EX1022 [zTrace How]; EX1019 [FAQ], 2; EX1013 [zControl How]; EX1026 [zControl PR]; EX1053; EX1028 [Yale PR]; *see* my opinions regarding limitation 1[c][iv] above. In my opinion, the claimed “**automatically disabling**” can occur “**in response to receiving**” either one of these “**notification[s]**.”

154. With respect to the notification being a disable request, upon receiving this notification, “**automatically disabling at least one user function of the mobile electronic device**” would be a logical next step, otherwise there is no reason to send such a request. *See, e.g.*, Isikoff, 6:17-30 (“The purpose of the low-level codes is to perform emergency functions under extreme circumstances.”). zTrace explains that the zControl application allows owners to “render the whole computer useless by locking its keyboard and mouse.” EX1053; *see also* EX1028 [Yale PR] (“render the computer useless by remotely locking all its functions”). These functions are understood to be the claimed “**at least one user function.**” Also, with respect to zTrace’s disclosures that “zControl... render[s] the device unusable,” i.e., zControl disables the laptop, a POSITA would understand that disabling a laptop or making

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

it unusable means that “**at least one user function**” is disabled. EX1026 [zControl PR]. If this were not the case, then the user would still be able to *use* the laptop. By its very definition, disabling a computer requires that “**at least one user function**” is disabled. Therefore, any disclosure in zTrace related to disabling the laptop also satisfies this element.

155. zTrace touts that the zControl application “provides automated control of a computer’s data.” A POSITA would have understood that this disabling occurs “**automatically**” as all actions taken by the zControl application on the laptop after the remote request is received are without user intervention. *See, e.g.*, EX1013 [zControl How], 1 (“zCONTROL... provides automated control of a computer’s data”); EX1026 [zControl PR], 1 (“zControl is stealth software that provides automated, remote and invisible control of the data stored on a computer”); EX1028 [Yale PR], 1 (“zControl... provides remote but invisible control of the data that is stored on the missing computer”); EX1053; *see also* Isikoff, 3:46-53, 4:3-14.

156. As an aside, even though the remote request is from the owner, and the actions taken by the zControl application on the laptop are in response to that request from the owner, it is my opinion that the user functions on the laptop are still “**automatically**” disabled. First, the user does not manually enter the disable request into the laptop itself – it is sent remotely from the web based user interface and

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

through the zServer to the zControl application. Second, the '649 patent describes similar embodiments where “[o]nce logged in, the user can report the device as stolen, [and] disable the device[.]” EX1001, 7:25-27. Even if Patent Owner argues that this does not constitute “**automatically disabling**,” other disclosures in zTrace support a narrower interpretation of this term.

157. As I previously discussed for limitation 1[c][iv], 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. *See, e.g.*, EX1013 [zControl How] (“[p]redefined actions,” including “retrieving files, [and] deleting sensitive information,” “can be triggered by... a zTRACE loss report”). 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. As previously discussed in connection with limitation 1[c], these applications work together cooperatively to provide the zTrace™ service. zTrace is silent with respect to the specific implementation of the predefined actions but such an implementation would have been well within the purview of a POSITA. The predefined actions would either be stored at the zServer or the laptop or preferably both – the options are limited based on zTrace’s disclosures. Indeed, as discussed for limitation 1[c][i],

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

Kesler indicates that its registration process includes sending “configuration values, software” and the “[c]onfiguration of the software,” which suggests to a POSITA that at least some of the information collected during registration is saved at the laptop. Kesler, FIG. 1. In my opinion, the predefined actions identified in zTrace would be used to configure the zTrace software and, in particular, the zControl application, so it would have been obvious for the predefined actions to be stored at the laptop and the zControl application configured to use / execute those actions based on instructions received from the zServer.

158. Also within the purview of a POSITA is that 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. In this obvious implementation, the zControl executes that action upon receiving the notification from the zServer.

159. For the same reasons discussed for limitation 1[c][iv], 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]. 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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

computer's data even AFTER loss has occurred" and "protect[] sensitive data in case of unauthorized access," respectively. EX1013 [zControl How]; EX1005 [zSecurity Suite page]. 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 require to disable the laptop.

160. As I also explained for limitation 1[c][iv], the predefined actions, including a "**notification**" to disable the laptop, can be sent from the zServer to the zControl application after the zServer receives notification that the laptop has been reported stolen. In this manner, the request to disable comes automatically from the zServer based on the preset instructions from the owner set during registration (or at some other point prior to the laptop being reported stolen). And, of course, as I mentioned before, "**automatically disabling**" features would have been a logical next step, otherwise there is no point to sending the request.

161. 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.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

This, again, would have been an obvious implementation of the zTrace applications for the reasons I discussed for limitation 1[c], which apply here.

162. 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.

163. It would have been obvious to maintain communication with the zServer after the 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. Specifically, as explained for that limitation, the zTrace™ service would have benefited from the laptop continuing to check in with zServer even after it receives notice of being reported stolen, as it would allow the laptop to provide its location (which would aid recovery if the laptop had been moved to a new location) and to regularly check for later-provided instructions from the laptop owner related to copying files, deleting

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

files, or disabling laptop functionality. EX1026 [zControl PR] (“Through the zControl web-based interface an owner of the missing computer can communicate with his/her computer ordering the remote and invisible deletion of files, recovery of data to the zServer and remote encryption of data... and can even render the device unusable”); EX1053. 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, for example, by enabling later-provided instructions for copying, retrieving and then deleting data from the laptop to be received and executed. *See* EX1013 [zControl How], 1 (“ZCONTROL... enables personal control of the computer’s data even AFTER theft or loss”). This would advance zTrace™ service’s objective to “protect[] sensitive data in case of unauthorized access[.]” EX1005 [zSecurity Suite page]. My opinions regarding limitation 1[c][iii] apply here.

164. Additionally, this configuration would advantageously allow the laptop owner to *first* disable certain features on the missing laptop to immediately prevent the thief from gaining access to sensitive data and *then* figure out how best to deal with the data still stored therewithin. If the laptop owner does not already have predefined actions set for handling data when there is a security breach, then the

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

disable-first, recover-second approach gives the owner more time to determine how best to recover data from the laptop while ensuring that the unauthorized user of the laptop cannot gain access to that data.

165. Furthermore, Isikoff's disclosures indicate that communication is still on-going even after certain features are disabled. For example, Isikoff discloses that "the beacon is activated... to enable or disable functions of the computer[.]" Isikoff, 1:59-65; *see also id.*, Abstract (similar language). A POSITA would know that a function must be disabled before it is enabled. So "to enable" a function means that that function is changed from a disabled state to an enabled state. The beacon receives the instruction to enable the function while the function is disabled so the beacon is still communicating with its remote server. Furthermore, the portions relied on here from Isikoff relate to disabling certain features, and not all features (like communication), so it would have been obvious for the communication functionality to be left on. *See* Isikoff, 2:12-20. It would have been obvious to implement this feature into zTrace for the reasons discussed above related to the benefits of maintaining communication with the zServer after the laptop and/or certain of its features are disabled. Indeed, zTrace is silent with respect to disabling communication with the zServer after the laptop and/or its features have been disabled.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

166. 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]: “automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;”**

167. zTrace discloses this limitation. As discussed throughout, the zControl application in zTrace executes predefined actions, including “retrieving files,” in response to a laptop being reported stolen. EX1013 [zControl How], 1 (“Action[s] can be triggered by... a ZTRACE loss report. Predefined actions can include retrieving files, [and] deleting sensitive information[.]”); EX1012 [zControl page] (“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. And, because the zControl application performs these predefined actions in response to the laptop being reported stolen, without any human intervention, the zControl application is 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 [zControl How]; EX1026 [zControl PR]; EX1028 [Yale PR]; EX1053.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

168. 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 (the owner can “order[] the... recovery of data to the zServer”). It is clear that “recovery” here refers to the data being “**copied from the mobile electronic device to at least one of the servers.**” The term “recovery” is used throughout zTrace to mean that data is returned to the owner, in the same way a lost laptop is recovered or returned to the owner. *See, e.g.*, EX1026 [zControl PR], 1 (“zControl is an invisible security application... that recovers files and deletes private information... after a computer has been lost[;]” “zControl... recovers files and deletes private information... after a computer has been lost[;]” “It can also be used by the owner to extract personal information saved in the computer[;]” “zControl... extract[s] data remotely”); EX1028 [Yale PR], 1 (“Through zControl, students will be able to remotely... recover specified files from their computers in case of loss or theft”); EX1005 [Suite page], 1 (“If your computer is out of your direct control, make the data invisible, encrypt it, recover it and then delete it”); EX1053. This is also how the term “recover” is used in the ’649 patent. *See* EX1001, FIG. 65 (“Data Recovery Service...If your phone is lost or stolen, this service will recover your Contacts, Calendar, and other key data (such as pictures) from your phone.”), 2:36-

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

37 (“recover data”), 9:3-23 (“Data Recovery Service—this service will allow a user to specify critical files and in the case of theft, the software will first recover these files to the ESTSM server”), etc.

169. The webpage [EX1053] and press release [EX1026] for the zControl application explicitly disclose that this data is recovered “to the zServer[.]” EX1053; EX1026. Although this statement is made in the context of sending remote instructions to the zControl application within a stolen laptop, a POSITA would have understood, or at least found it obvious, that this copying functionality to the zServer 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. *See, e.g.,* Isikoff, 8:22-61 (disclosing similar copying functionality performed by predefined actions). In other words, the zControl application is understood to perform the same copying functionality on the laptop regardless of whether it was instructed via remote control or predefined action. *See supra*. In all instances, the data is copied to the zServer so that the laptop owner can recover the data.

170. Other zTrace disclosures support my conclusion. For example, as will be discussed, the zTrace zSecurity Suite webpage [EX1005], which has a June 2002 capture date, states: “If your computer is out of your direct control, make the data

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

invisible, encrypt it, recover it and then delete it.” EX1005. This sequence indicates recovering first and then deleting. A POSITA would know that recovery here means that the data is copied from the computer and then the original data remaining on the computer is deleted so an unauthorized user cannot gain access to it. The zServer is the most logical place to store the recovered data. For this reason alone, the zTrace disclosures relating to recovering data to the zServer are understood to apply to data recovered via predefined actions.

171. As discussed for previous limitation 1[c][v], the steps the zControl application executes to carry out the predefined actions, including the copying functionality, are automated, and do not require any human intervention to complete. *See supra*. Thus, the zControl application “**automatically caus[es] at least some user data to be copied from the mobile electronic device to at least one of the servers.**”

172. Isikoff further evidences the above functionality in zTrace. Isikoff describes similar options for copying data from a laptop to a server associated with the service provider in response to a laptop being reported missing. For example, Isikoff describes an owner-initiated option where, “when the computer is stolen, the user determines whether there are any critical files which must be recovered whether the machine is found or not” and “[t]he user sends a broadcast [to the laptop] to

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

initiate transfer of these files.” Isikoff, 8:22-45. Isikoff explains that “[t]his is done... through a central clearing house service center, which may for example be operated by a computer security company... to receive and temporarily store such data[.]” *Id.* (also discloses that “[u]pon receipt of the lower level codes, the document recovery request is treated as a priority task and the codes are executed as soon as possible, resulting in the transmission of the vital files back to the owner”). Isikoff also describes an option where “the application software itself determines which files need to be transmitted” “without the intervention of the user.” Isikoff, 8:46-61. A POSITA would have understood, or at least found it obvious, that the central clearing house service center where the recovered data is temporarily stored includes a server. It would have been normal to use a file server for this purpose or even an FTP server that itself contained a file server.

173. In my opinion, it would have been obvious to combine the general teachings of Isikoff with zTrace because doing so would predictably result in the zControl application using predefined actions to copy select files and data from the missing laptop to the zServer as a part of the recovery process. zTrace provides teachings, suggestions and motivations for this modification. As just discussed, zTrace describes instances where an owner can use a zControl web based user interface to send instructions to the stolen laptop (and in particular the zControl

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

application on that laptop) to recover data “to the zServer.” *See supra*. A POSITA would have been motivated to look to references, like Isikoff, for more details regarding this copying process and how it can be implemented when predefined actions are executed. And, indeed, Isikoff indicates that the copying functionality is executed in the same manner regardless of where the instructions came from.

174. A POSITA would have further found it obvious to try combining Isikoff with zTrace because Isikoff is an analogous reference, as discussed for limitation 1[c][v], and their disclosures regarding the copying process are so similar. For example, like Isikoff, zTrace discloses an option where the owner remotely controls what data is recovered (or “copied”) and an option where the user can predefine what data is recovered in the event the laptop is reported missing. EX1013 [zControl How]; EX1026 [zControl PR]; EX1053. In both instances, as explained above, the zControl application performs the recovery automatically within the laptop without any human intervention. *See supra*. It would have been obvious for the zServer to act in the same manner as the central clearing house service center in Isikoff, which is understood to be effectuated by a server, to receive the copied data, as the zServer is the only component in the zTrace™ service that appears to communicate directly with the laptop. The zServer, therefore, would be a logical place to receive and/or store (at least temporarily) the recovered data from the laptop. For these reasons,

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

such a combination would have been trivial to implement and would have every reasonable expectation of success.

175. Limitation 1[c][vi] is therefore rendered obvious by zTrace alone and zTrace in view of Isikoff.

(j) Limitation 1[d]: “wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;”

176. Non-volatile memories were ubiquitous by August 2003, as discussed in my technology overview. Breaking this term down, a “memory” is “[t]he part of a computer... which stores information or instructions for use.” EX1037, 433. “Non-volatile” is defined as “[m]emory which is not lost... when the power is shut off.” EX1037, 481. The ’649 patent defines “non-volatile memory” consistent with its use in the art: “a ‘nonvolatile’ memory device... means that the memory contents remain intact even when the computer 4900 powers down.” EX1001, 22:13-18. Thus, the claimed term “non-volatile memory” is subject to its plain and ordinary meaning as it would be understood by a person with ordinary skill in the art.

177. A hard drive is a non-volatile memory because it is memory that persists after powering down. I understand from counsel that, in its infringement contentions, Patent Owner confirmed that a hard drive is memory. EX1036, 56. The

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

zTrace laptop includes a hard drive (i.e., a “2M HD”). EX1019 [FAQ], 2. Therefore, zTrace discloses a “**non-volatile memory**.”

178. To the extent Patent Owner argues a construction for “**non-volatile memory**” that excludes a hard drive, then this limitation is generally disclosed by Bonnett. (Note that I discuss Bonnett in more detail in the next sections but, for purposes of this limitation, I discuss Bonnett at a high-level.) 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] (explaining the “technical advantages” of securing a program), [0019], [0024]. The device in Bonnett includes a memory 124 for this purpose that may be “a NAND flash memory, or any other suitable volatile or nonvolatile storage and retrieval device or combination of devices.” Bonnett, [0031]. The “NAND Flash memory” is a specific type of flash memory that is used in mobile devices by August 2003. This last disclosure of “any other suitable... nonvolatile storage and retrieval device” is broad enough to include any of the nonvolatile memories I mentioned in my technology background, which were all known in the art by August 2003, including other types of flash memory (besides NAND flash memory).

179. For context, the '649 patent describes embodiments where the non-

108

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

volatile memory is a “flash memory” generally. *See* 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”). This could refer to NAND flash memory or other types of flash memory. The disclosures are not specific.

180. Turning back to the prior art, 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 other type of “nonvolatile storage and retrieval device,” in addition to the hard drive. 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 [FAQ], 2; *see also* Isikoff, FIG. 4 (showing a computer schematic with a “Memory,” “Disk or CD Drive,” and a “Hard Drive”); Cotichini, FIG. 8C (illustrating a computer with Flash EPROM and multiple RAM), 3:18-44 (describing multiple types of memory on a computer, including a hard disk, ROM BIOS, Flash ROM, etc.). The Intel processor in zTrace’s laptop was specifically designed to operate with multiple types of memories as well. *See* EX1035, 22-23 (describing “[m]emory [o]rganization” including “physical memory” and “virtual memory”), 26 (explaining the use of “RAM,” “disk storage,” and “ROM”), 29 (Figure 5-1, identifying physical memory such as “EPROM” and “DRAM”), etc.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

181. Adding an extra memory component to zTrace's laptop would allow the laptop to store more programs and provide enhanced functionality to the owner. *See* EX1038 [Windows XP Unleashed], 24 ("A disk drive with 5MB to 10MB of storage capacity was once considered enormous, but now a 60GB or larger hard drive is not only the norm but also available for a very low cost."). Adding another memory component to the laptop would have been a relatively easy feat for a POSITA as most laptops were equipped with extra space for additional cards and components, and the modification would involve using off-the-shelf components that were already technologically compatible with each other. Thus, this modification could be accomplished with a reasonable expectation of success, without any change in functionality to the hard drive or other components.

182. 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. As will be discussed in more detail for limitation 1[f], the flash memory would have further been capable of storing the zTrace applications.

183. zTrace would have also benefited from an additional memory component – either a flash memory or other nonvolatile memory – because that

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

additional memory could have served as a long-term backup space for storing a copy of the zTrace applications or vice versa, as discussed in more detail in the next sections. It was common at the time to have backup copies of programs, especially critical programs, within the computer to avoid a single point failure. For example, Cotichini discloses that its similar tracking and recovery software agent “may be installed in a variety of locations whereby second and third agents can provide back up support for the primary agent.” Cotichini, 18:15-33. As will be discussed in more detail for limitation 1[f], a backup copy of the applications would be particularly useful if the laptop is stolen and some of its parts are stripped, including one of the components that stores the applications. Again, this is addressed in more detail below.

184. Including an additional memory component was an obvious design choice. The components in the zTrace laptop (e.g., RAM, hard drive, Intel processor) are off the shelf components that existed prior to August 2003 (*see* my opinions for limitations 1[a] and 1[b]) and it was well known that they could be used interchangeably or together, with predictable benefits (including those mentioned above). *See, e.g.,* Forbes, 1:35-44 (a 1997 patent explaining: “Flash memories have the potential of replacing hard storage disk drives in computer systems. The advantages would be replacing a complex and delicate mechanical system with a

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

rugged and easily portable small solid-state non-volatile memory system.... Flash memories might then have the ability to fill all memory needs in future computer systems.”).

185. Flash memory was very popular by August 2003, especially for use in mobile devices, such as laptops. Bez [EX1046] – a white paper describing flash memory technology – explains that “[i]n the late 1990s, the Flash technology exploded as the right non-volatile memory for code and data storage, mainly for mobile applications.” Bez, 491. “Starting from 2000, the Flash memory can be considered a really mature technology[.]” *Id.*; *see also id.*, 490 (“The most relevant phenomenon of this past decade in the field of semiconductor memories has been the explosive growth of the Flash memory market, driven by cellular phones and other types of electronic portable equipment (palm top, mobile PC, mp3 audio player, digital camera, and so on).”); Goronkin, 806 (“Flash memory [is] a highly successful commercial nonvolatile memory”).³ A POSITA would have been

³ I note, as I did in my technology tutorial section above, that the Goronkin paper appears to have published in November 2004, which is after August 2003. I can confirm, however, that the content in this paper was known well before August 2003

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

motivated to try implementing a flash memory into zTrace's hard drive for this reason alone. A POSITA would have also found the addition of flash memory to be an obvious design choice for this reason as well.

186. A POSITA would have been motivated to look 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 [FAQ], 2 (“There are no icons, files, directories, sounds or ANYTHING visible on the computer, providing total invisibility to the user”); EX1007 [Gold Brochure] (“ZTRACE GOLD is undetectable and unerasable on a laptop's hard drive”); EX1013 [zControl How] (“ZCONTROL is an invisible software application”). 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 Patent Owner provides a narrow construction that excludes a hard drive as a non-volatile memory. Again, nonvolatile memory was the only type of memory that could provide long-term

and any POSITA would attest that flash memory was commercially successful prior to August 2003.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

storage of the zTrace applications and there were only a finite number of nonvolatile memories available by August 2003 – a flash memory was one of them. Additional motivations to combine these two references are discussed in connection with limitations 1[e] and 1[f] and apply here. For all these reasons, this combination would have at least been obvious to try and would have yielded predictable results.

187. Additionally, 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. Isikoff is relied on for the limited purposes of teaching disabling laptop features, which would not be impacted by including additional memory in the zTrace laptop.

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

(k) Limitation 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;”

189. As discussed in the technology background section above, it was

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

common for memory to include secure areas that could only be accessed with certain privilege levels. (The discussions in that section are incorporated by reference here.)

190. The terms “changeable area” and “system area” were not well-known terms of art but a person of ordinary skill would have understood them to refer to areas within memory that were not hidden and hidden, respectively. The ’649 patent refers to a “changeable area” and a “system area” in reference to Figures 45 and 48, which are illustrated side-by-side below.

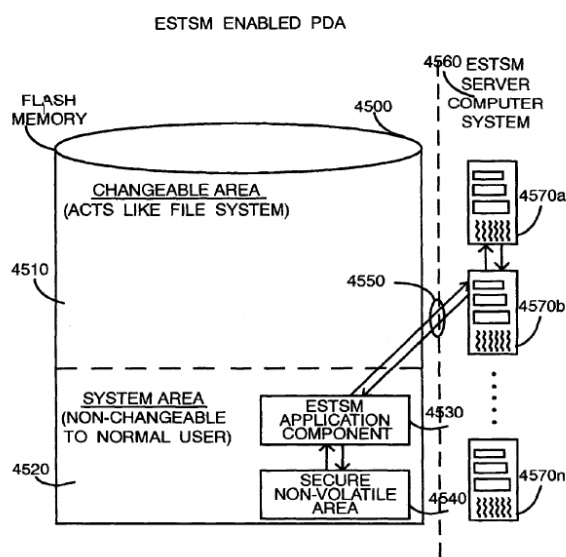


FIGURE 45

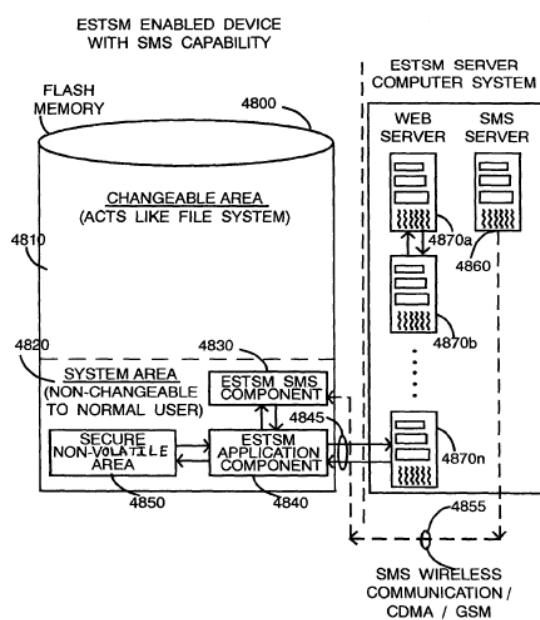


FIGURE 48

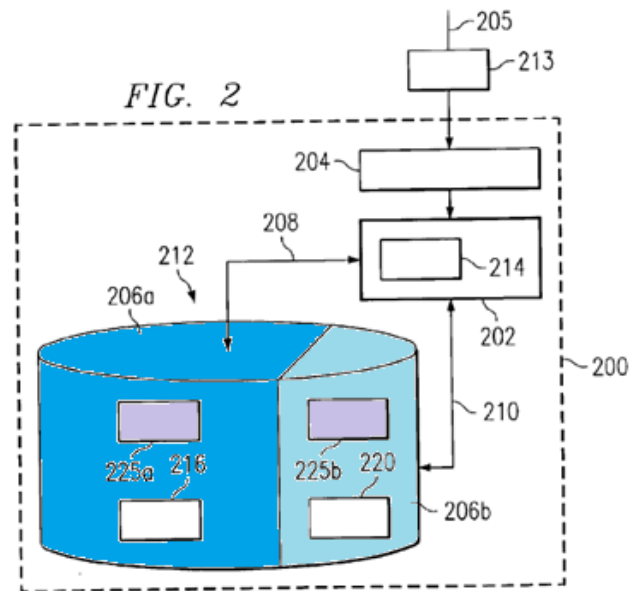
191. Looking first to the “system area,” the figures indicate that this area is “non-changeable to [a] normal user.” The specification further describes this area as “non-viewable.” EX1001, 3:48-49 (“The system area is not changeable by the user

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

of the electronic device”), 19:16-18 (“[T]he system area 4520 may be non-viewable and implemented in non-volatile memory.”), 20:17-21 (“A system area 4820... that is non-changeable to a user of the electronic device”). Note that the figures above reference a “normal user.” I discussed this type of user previously with respect to limitation 1[c].

192. Looking next to the “changeable area,” the figures indicate that this area “acts like [a] file system.” EX1001, 20:14-17 (“The electronic device may include a Flash memory 4800 containing a changeable area 4810 that functions like non-volatile storage and may include a file system.”). The changeable area would be an area that is not hidden and one that a user can freely access.

193. This limitation is rendered obvious based on the combined disclosures of zTrace and Bonnett, regardless of how Patent Owner interprets “**non-volatile memory**.” Bonnett discloses that its memory, which can be “a NAND flash memory, or any other suitable... nonvolatile storage and retrieval device[,]” Bonnett, [0031], [0035], includes an “open partition” and a “hidden partition,” Bonnett, [0036]. This configuration is shown below in Figure 2 of Bonnett, which has been annotated to identify the open partition (206a) of the nonvolatile memory (212) in dark blue and the hidden partition (206b) in light blue.



The open partition (206a) stores “media files, data files, and/or any other information desired by program designers to be accessible to the user[,]” (represented as 225a in purple above). Bonnett, [0036]; *compare to* EX1001, FIG. 45 (the “changeable area” “acts like [a] file system”). The hidden partition stores “executable files, the operating portion of the program, operating system applications... firmware, 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.

194. 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” and can therefore be modified by a user. The hidden partition described in Bonnett acts as a

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

“**system area that cannot be modified by the user**,” because that partition is “made inaccessible to [the] user.” Another term for “hidden” is “non-viewable.” *See* EX1001, 19:16-18. And if an area is “inaccessible” it means that it cannot be modified.

195. I understand from counsel that this interpretation of the “**changeable area**” and the “**system area**” is consistent with Patent Owner’s application of these claim terms in its infringement contentions in the parallel district court litigation. For example, for this limitation, Patent Owner 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 [a]pplication agent is not changeable by a user and therefore resides at least partially in the system area.” *Id.* This is what is described in Bonnett. As alluded to for limitation 1[c] and as will be discussed in more detail below, this is also what is described in zTrace.

196. In my opinion, 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 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. In this manner, the hard drive in zTrace would explicitly include the

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

claimed “**changeable area**” and “**system area.**”

197. zTrace provides teachings, motivations and suggestions to combine with Bonnett in this manner. 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 [Gold Brochure]. An application that is “undetectable” on a hard drive is understood to be hidden on the hard drive. 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. To achieve these characteristics, the hard drive in zTrace would have been understood to include a hidden or otherwise secure area in which the zTrace Gold is stored. Patent Owner confirmed this in its infringement contentions – 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. zTrace clearly restricts access to the zTrace Gold application and therefore, according to Patent Owner, the application must reside in a system area of the hard drive. *See* EX1019 [FAQ], 2 (“zTrace Gold is an invisible software application”), 2 (“There are no icons, files, directories, sounds or ANYTHING visible on the computer, providing total invisibility to the user”), 3 (“zTrace operates totally undetected”); *see also* Kesler,

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

[0017] (confirming that a portion of the client software is “installed onto track zero” of the hard drive, which is known to be a hidden track on the hard drive).

198. zTrace also suggests that the zControl application is stored in a hidden area, although it is silent as to which memory component includes this hidden area and thus where in the laptop the zControl application is stored. But, as I discussed for limitation 1[c], it would have been obvious for the zControl application to be stored in the hard drive. *See* my opinions for limitation 1[c] above. As I noted, zControl is also described as an “invisible software application[.]” EX1013 [zControl How]; *see also* EX1026 [zControl PR]; EX1053. An application that is invisible is undetectable or “hidden” and thus, for the same reasons I just discussed, a POSITA would have understood that the zControl application is also stored in a hidden or otherwise secure area that is non-viewable to the user.

199. As an aside, the zControl application is not described as being “unerasable” like the zTrace Gold application. But, in my opinion, this does not matter. The zControl application is otherwise described in the same way as the zTrace Gold application – it is invisible. *See also* EX1026 (“zControl provides a stealth solution”). Meaning, access to this application is hidden or restricted. And, as I mentioned above, Patent Owner finds this to be enough to demonstrate a system area. When zTrace is combined with Bonnett, this “**system area**” is clear.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

200. With respect to the claimed “**changeable area**,” this is not expressly disclosed in zTrace; however, the changeable area is simply the opposite (for the most part) of the system area. For example, according to Patent Owner, it is an area that is not restricted and “provide[s] access to certain files (e.g., files stored in a changeable area)[.]” EX1036, 59. A POSITA would understand that zTrace’s hard drive would include such accessible areas, as not all areas of a hard drive are hidden. Again, when zTrace is combined with Bonnett, this “**changeable area**” is clear.

201. 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]. A hard drive is nonvolatile, it provides storage and data can be retrieved from it. It is thus a nonvolatile storage and retrieval device. Thus, a POSITA would have been motivated to look to Bonnett for details on how the hard drive in zTrace’s laptop could be configured and where on the hard drive the zTrace Gold and zControl applications should be located so they remain hidden from the user.

202. Bonnett also enumerates the “technical advantages” of restricting access to programs stored in memory. It explains that “[r]estricting access to programs and/or portions of a program can help prevent a user from deleting or

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

corrupting those portions of the program, which can lead to an improved reliability of the appliance [e.g., laptop].” Bonnett, [0011]. This is precisely why zTrace requires its applications to remain “invisible” – so that an unauthorized user cannot alter or delete the applications on the laptop and gain access to the potentially sensitive data stored on the laptop. A POSITA would have known that these technical advantages align with the purpose of zTrace.

203. For all of these reasons, it also would have been obvious to try combining Bonnett with zTrace. It would have been obvious to look to Bonnett for more explicit disclosures of the hidden area (“**system area**”) already suggested in zTrace. And, as I previously discussed, 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. Any modification to zTrace would have therefore been trivial and would have had every expectation of success.

204. 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. As discussed above, hard drives were already known to have hidden partitions so choosing a particular hard drive known to have a feature

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

that would benefit the zTrace applications would have been obvious.

205. 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.

206. 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.”**

207. 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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

memory component within the modified zTrace laptop to include a hidden partition and an open partition. Bonnett, [0007], [0031]-[0037]. As I mentioned above for limitation 1[d], adding another memory component in zTrace's laptop has its benefits, including extra memory space and a location to store a backup copy of the zTrace Gold and zControl applications (or store the main versions of those applications and the hard drive acts as the backup storage location). Most laptops by August 2003 included multiple memory components, including multiple nonvolatile memory components, which provided long term storage solutions for laptops and any programs running on those laptops. The zTrace laptop also included an Intel processor that was well suited for handling multiple of these memory components. This modification would have been trivial and would have every expectation of success. It would have also been obvious to try as well as an obvious design choice for the reasons previously discussed.

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.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

(l) **Limitation 1[f]: “wherein the security application utilizes code residing at least partially in the system area; and”**

209. The combined disclosures of zTrace and Bonnett render this limitation obvious.

210. In instances where the “**non-volatile memory**” includes a hard drive, it would have been obvious to a POSITA to combine zTrace and Bonnett based on my 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]. 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 [Gold Brochure]; EX1013 [zControl How]; EX1026 [zControl PR]; EX1053; EX1019 [FAQ], 2 (“zTrace Gold is an invisible software application”), 2 (“There are no icons, files, directories, sounds or ANYTHING visible on the computer, providing total invisibility to the user”), 3 (“zTrace operates totally undetected”); *see also* Kesler, [0017] (discussing installing a portion of the client software on “track zero” of the hard drive, which is known to be a hidden track). My opinions for limitations 1[c], 1[d] and 1[e] apply here.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

211. A POSITA would have understood that the processor-executed “applications” in zTrace include “**code.**” It was well known that processors, including zTrace’s 386 DX Intel processor, only execute code and that applications are comprised of code. EX1035, 5-1 (describing an application with “instruction code” that is executed by the Intel 386 DX processor), 1-1, 2-1; *see, e.g.*, Bonnett, [0019] (programs include “code [or] portions of code”); Cotichini, FIG. 14H (identifying “agent code” stored on the hard drive); Cheston, 1:8-11 (describing “a hidden partition in its disk storage to store code”), 2:16-19; Dayan, [0001] (describing “a designated partition in a non-volatile storage unit storing code to conduct recovery/maintenance operations”); Bez, 490 (describing “code storage, where the program or the operating system is stored and is executed by the microprocessor or microcontroller”). Thus, if the claimed “**non-volatile memory**” includes a hard drive, then zTrace in view of Bonnett discloses “**wherein the security application utilizes codes residing at least partially in the system area.**”

212. 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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

“undetectable” to the laptop user. A POSITA would have understood that the processor executes applications the same way regardless of where the applications are stored in the laptop. For example, Intel’s 386 processor uses the same memory management paging technique for all memory. EX1035, 2-1. 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. This combination could therefore be achieved with a reasonable expectation of success.

213. 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. Also, it would have been obvious to try installing the zTrace™ applications on an additional memory component to free up space in the hard drive for storing other data or it could also be the case that the hard drive’s memory is already full so installing onto an additional memory component is necessary to effectuate the applications on the laptop. *See, e.g.*, EX1038 [Windows XP Unleashed], 24 (“A disk drive with 5MB to 10MG of storage capacity was once considered enormous, but now a 60GB or larger hard drive is not only the norm but

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

also available for a very low cost.”). Again, 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.

214. 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 (discussing “where computers are stripped for parts” tracing software can still be used “even if a new disk drive is installed” because the tracing software is stored elsewhere in the laptop). 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. 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.

215. For this same reason, as I mentioned for limitation 1[d], a POSITA would have understood the benefit of storing backup copies of the zTrace

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

applications within the additional memory component in case the hard drive is stripped from the laptop, ensuring that the zTrace™ service persists even if the hard drive is removed from the laptop. The opposite would have also been beneficial – the main zTrace applications could be stored on the additional memory component within the zTrace laptop and backup copies of the applications could be included in the hard drive. This type of configuration was well known in the art. *See* Cotichini, 18:15-33.

216. As I also mentioned for limitation 1[d], flash memory, in particular, was very popular by August 2003 and was frequently used to store programs in mobile devices. *See* Bez, 489-491; Goronkin, 806. It was even contemplated that hard drives could be *swapped out* for flash memory in mobile devices as there were numerous benefits of flash memory over hard drives. For example, Forbes – a 1997-filed patent – explains that “[f]lash memories have the potential of replacing hard storage disk drives in computer systems.” Forbes, 1:35-44. “The advantages would be replacing a complex and delicate mechanical system [i.e., the hard drive] with a rugged and easily portable small solid-state non-volatile memory system [i.e., flash memory].” *Id.* Bonnett discloses that such flash memories have hidden partitions. A POSITA would understand that these partitions would have been suitable for storing the zTrace applications for these reasons and those above. Storing the zTrace

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

applications in the hidden areas of the flash memory would have been an obvious design choice given the popularity of flash memory in mobile devices by August 2003. It also would have been obvious to try modifying zTrace in this manner.

217. 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 or the location in which the application is stored because, as I discussed above, the Intel processor in zTrace’s laptop executes the application code in the same way.

218. For these reasons, zTrace in view Bonnett renders this limitation obvious.

(m) Limitation 1[g]: “wherein the security application receives the notification from at least one of the servers via the system area.”

219. The claimed “**notification**” here first appears in limitation 1[c][iv]. For that limitation, I 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 [Gold Brochure]; EX1022 [zTrace How]; Kesler, [0017], claim 10. I 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 [zControl How]; EX1026 [zControl PR]; EX1028 [Yale PR]; EX1053; 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.**”

220. 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 4870*a*, 4870*b*,... 4870*n*... through an Internet connection 4845.” EX1001, 20:8-31, FIG. 48; *see also*

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

id., 19:8-26 (similar description), 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. I understand from counsel that this is consistent with how Patent Owner 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.

221. It is my opinion that, 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 Patent Owner’s interpretation of this claim limitation, a POSITA would have understood that the applications receive the notification “**via the system area.**” The applications in zTrace, as modified by Bonnett, reside in similar locations within the laptop as the corresponding software in the ’649 patent and function in a similar manner to that software. And, therefore, when subjected to the same conditions as the software in

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

the '649 patent, a POSITA would understand that the zTrace applications operate and receive notifications in the same way. Limitation 1[g] is thus satisfied.

222. 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, e.g.*, 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] (storing programs within a hidden memory partition is "advantageous" because it "substantially prevent[s] a user from deleting and/or corrupting those... program[s]."); EX1007 ("zTRACE GOLD is undetectable and unerasable on [the] laptop's hard drive."); EX1013 (zControl is described as an "invisible software application"); EX1026; EX1053; EX1019, 2-3; Kesler, [0009] ("The software is difficult to detect on the computer being traced;" "Because the tracing software [operates] without any prompt or alert, the user (a thief or person in possession of a stolen computer) is unaware of and unable to stop the process."),

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

[0017] (the client software is “installed onto track zero” of the hard drive; “[T]he software will download invisibly and install itself, which significantly reduces the opportunity for tampering”); *see also* my related opinions for limitations 1[e] and 1[f]. If communications are not protected or concealed, the zTrace™ service would be rendered useless because the unauthorized user of the stolen laptop would become aware of the security software as soon as communication occurred and could delete or disable the communication functionality, rendering the zTrace service inoperable to achieve its intended purpose of allowing laptop owners to recover laptop data and hardware that has been lost or stolen.

223. To the extent Patent Owner interprets this limitation inconsistent with the '649 patent disclosures or of its application of this claim element in the parallel district court litigation, I reserve the right to request a reply to address that new interpretation and/or reserve the right to revise its prior art combination to address this new interpretation.

224. 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].

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

2. Independent claim 9

226. 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. Below is a complete side-by-side comparison of claim 9 to claim 1 with additions underlined and deletions in strikethrough.

Claim 9 limitations	Claim 1 limitations
9.[pre] <u>A method for providing security for a mobile electronic device, the method comprising:</u>	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:~~
9[a] <u>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;</u>	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;
9[b] <u>in response to the request from the owner, registering the mobile electronic device with the security service;</u>	
9[c] <u>automatically sending identifying information for the mobile electronic</u>	1[c][ii] ~~causing the mobile electronic device to~~ automatically send identifying

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

device from the mobile electronic device to the security service;	information for 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;	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;
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;	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;
9[f] in response to <u>accepting</u> 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][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
9[g] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;	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;
9[h] <u>wherein the mobile electronic device</u> comprises non-volatile memory;	1[d] ~~wherein the one or more non-transitory machine-readable storage media~~ comprises non-volatile memory;
9[i] wherein the non-volatile memory comprises a changeable area that can be	1[e] wherein the non-volatile memory comprises a changeable area that can be

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

modified by a user and a system area that cannot be modified by the user;	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	1[f] wherein the security application utilizes code residing at least partially in the system area; and
9[k] <u>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.</u>	1[g] ~~wherein the security application~~ receives the notification from at least one of the servers via the system area.

227. As indicated above, 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. Claim 9 only recites a security application with respect to later limitation 9[j] and that application functionality is not tied to any of the functionality recited in the previous limitations, like it is for claim 1. Also, method claim 9 does not recite “**a processor**” or “**one or more non-transitory machine-readable storage media responsive to the processor.**”

228. I only address the preamble and limitations 9[a] and 9[b] below because they differ the most from claim 1. As stated above, the remaining limitations are substantively identical to those in claim 1 and therefore my opinions for those claim 1 limitations apply here to the corresponding claim 9 limitations.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

(a) **Preamble: “A method for providing security for a mobile electronic device, the method comprising:”**

229. To the extent the preamble of claim 9 is limiting, it is disclosed by zTrace. For example, zTrace discloses implementing security software in “laptop computers,” which are “**mobile electronic device[s]**.” EX1019 [FAQ], 2 (“zTrace™ will run on Desktop and Laptop Computers”); EX1006 [Gold] (“an invisible software security application that traces the location of missing laptops for recovery”). 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 [Suite page]. Thus, zTrace discloses “[a] **method for providing security for [the] mobile electronic device.**”

(b) **Limitation 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;”**

230. For the same reasons I discussed for limitation 1[c][i], zTrace discloses that “**an owner of the mobile electronic device [] register[s] the mobile electronic device with a security service residing at least partially on one of more servers.**” *See, e.g.*, EX1004 [Overview], 1 (“Welcome to zTrace! ... Register Now!”);

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

EX1019 [FAQ], 2, 3; EX1007 [Gold Brochure].

231. Limitation 9[a] adds “**receiving, at a mobile electronic device, a request from [the] owner... to register.**” In my opinion, this is an obvious feature because an owner generally has to request registration and fill out the required information to enable registration. That said, it is obvious that the owner would use her laptop to complete the registration for the zTrace™ service by inputting commands into the laptop instructing the laptop to commence the registration process. *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, shown in excerpt and annotated below, which includes a “Register Now!” link.



EX1004 [Overview] (excerpt). A POSITA would have understood that a simple

click on the “Register Now!” link would have resulted in the laptop **“receiving... a request from [the] owner... to register”** the laptop.

232. A POSITA would have further understood that otherwise initiating or completing the registration would also equate **“receiving... a request from [the] owner... to register”** the laptop. For example, as discussed for limitation 1[c][i], the owner can actuate a “registration and installation wizard” on his or her computer as part of the registration process. *See, e.g.*, EX1019 [FAQ], 2 (“How do I install zTrace?... [F]ollow the registration and installation wizard on the zTrace web site”), 3 (“Just resubmit your registration, and your new computer will be zTrace™ protected too.”). Thus, zTrace renders this limitation obvious.

(c) Limitation 9[b]: “in response to the request from the owner, registering the mobile electronic device with the security service;”

233. 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. 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 [FAQ], 3. The submission here

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

acts as the “**request**” and the subsequent laptop protection is what happens after
“**registering the mobile device with the security service.**”

234. Similarly, a POSITA would know that completing the registration and installation wizard would predictably result in the zTrace’s laptop being registered with the security service. EX1019 [FAQ], 2 (“How do I install zTrace?... [F]ollow the registration and installation wizard on the zTrace web site”). As explained in zTrace, the zTrace Gold application “is installed on the laptop’s hard drive and registered with the ZSERVER[.]” EX1007. Using the wizard to install the application results in the application being registered with the server.

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

3. Dependent claims 7 and 15

236. Claim 7 depends from claim 1 and claim 15 depends from claim 9. Each recite in relevant part:

Claim 7	Claim 15
<u>wherein the operations the security application is operable to perform further comprise:</u> 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	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

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

the user data to be deleted from the mobile electronic device	
---	--

237. 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 [Suite page]. Thus, zTrace discloses that files and data can be first “**copied**” (i.e., recovered) from the laptop and then “**deleted**” from the laptop. *See* my opinions for limitation 1[c][vi] addressing copying user data to the zServer, which apply here.

238. As I also discussed for limitation 1[c][vi], this same sequence can be implemented when predefined actions are executed. “Predefined actions can include retrieving files [and] deleting sensitive [user] information.” EX1013 [zControl How]. 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.*

239. 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.*, EX1026 [zControl PR] (“zControl is an invisible security application... that recovers files and deletes

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

private information... after a computer has been lost[;]” “zControl... recovers files and deletes private information... after a computer has been lost[;]” “zControl is able to delete information upon loss of the computer”); EX1053 (“zControl... deletes sensitive information”); EX1028 [Yale PR] (“Through zControl, students will be able to remotely... delete[] and recover specified files from their computers in case of loss or theft”); EX1013 [zControl How] (“ZCONTROL is an invisible software application that provides automated control of a computer’s data... includ[ing] retrieving files [and] deleting sensitive information”).

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

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

241. 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, (73); EX1019 [FAQ], 2 (zTrace “run[s] on Desktop and Laptop Computers with... 386 DX or higher”); EX1035 [386 DX Textbook], 1 (“386™ DX Programmer’s Reference Manual”). As I mentioned before, I am very familiar with the Intel 386™

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

processor and its functionality. All other arguments under Ground 1 remain the same and are incorporated by reference into Ground 2.

1. **Limitation 1[d]: “wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;”**

242. As discussed for limitation 1[d] under Ground 1, zTrace discloses a hard drive that is the claimed “**non-volatile memory**.” *See* EX1019 [FAQ], 2; EX1036, 56; EX1037 [Newton 17 dictionary], 481; EX1001, 22:13-18.

2. **Limitation 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;”**

243. As discussed in the technology background section above, it was common for memory to include secure areas that could only be accessed with certain privilege levels. The discussions in that section are incorporated by reference here. Also incorporated here is my analysis of the ’649 patent set forth at the outset of limitation 1[e] under Ground 1.

244. In my opinion, 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*

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

EX1007 [Gold Brochure] (“zTRACE GOLD is undetectable and unerasable on [the] laptop’s hard drive”); EX1019 [FAQ], 2 (“zTrace Gold is an invisible software application”), 2 (“There are no icons, files, directories, sounds or ANYTHING visible on the computer, providing total invisibility to the user”), 3 (“zTrace operates totally undetected”); EX1013 [zControl How] (identifying zControl as an “invisible software application”); EX1026 [zControl PR] (similar); EX1053. But zTrace falls short of affirmatively identifying those hidden or secure areas. Eckardt, however, provides these disclosures.

245. 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. In other words, that partition can be modified by a user. This partition therefore acts as the claimed “**changeable area that can be modified by the user.**” 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, 4:52-59, 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**

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

modified by the user.” I have been advised by counsel that this interpretation of the “**changeable area**” and the “**system area**” is consistent with Patent Owner’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. *See* EX1036, 59.

246. In my opinion, 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**”). As just discussed, zTrace’s disclosures provide the teaching, suggestion and motivation for this combination and hard drive configuration because its applications are “invisible” and this necessitates a hidden partition on the hard drive. *See* EX1007 [Gold Brochure]; EX1019 [FAQ], 2-3; EX1013 [zControl How]; EX1026 [zControl PR]; EX1053. My opinions regarding these disclosures under Ground 1 apply here.

247. 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. I discuss these partitions in my technology background section as well. I do not refer to them as “legal” or “illegal”

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

– that is just nomenclature. Because partition hard drives were so well known, a POSITA would have understood how to implement these partitions in zTrace’s hard drive with a reasonable expectation of success. It also would have been obvious to try combining zTrace with Eckardt so that zTrace has similar partitions for the same reasons.

248. A POSITA would have been motivated to seek more information about how to implement hidden areas within the hard drive to keep the zTrace applications “invisible” to the end user for the same reasons discussed under Ground 1. A POSITA would have been particularly motivated to look to Eckardt for these details because it is a patent from Intel Corp. and, as discussed for limitation 1[a] under Ground 1, the zTrace laptop includes a 386™ DX processor by Intel. Eckardt, (73); EX1019 [FAQ], 2; EX1035, 1 (“386™ DX Programmer’s Reference Manual”). 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. A POSITA familiar with hard drives would have understood that it was simple to leave areas of the hard drive unallocated to the operating system. These areas would be invisible to the operating system and would have been a secure place to store hidden information.

249. For the same reasons discussed for this limitation under Ground 1, a

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

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]. It would have been obvious to try combining Eckardt with zTrace for these reasons.

250. 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] (disclosing installing a portion of the client software on “track zero” of a hard drive, which is known to be a hidden track). 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.

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

3. Limitation 1[f]: “wherein the security application utilizes code residing at least partially in the system area; and”

252. 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*. To the extent they collectively form a single application, that single application would reside in the hard drive. *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 [Gold Brochure]; EX1013 [zControl How]; EX1026 [zControl PR]; EX1053; EX1019 [FAQ], 2 (“zTrace Gold is an invisible software application”), 2 (“There are no icons, files, directories, sounds or ANYTHING visible on the computer, providing total invisibility to the user”), 3 (“zTrace operates totally undetected”). As discussed for limitation 1[f], the zTrace applications are comprised of code. *See* my opinions for limitations 1[e] and 1[f] under Ground 1 to the extent they are applicable. 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.

4. Limitation 1[g]: “wherein the security application receives the notification from at least one of the servers via the system area.”

253. 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 Patent Owner’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.

254. 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). Consistent with the disclosures in the ’649 patent and the Patent Owner’s application of this limitation in its infringement contentions, these applications are therefore understood to receive the notification from the zServer **“via the system area.”** The applications in zTrace, as modified by Eckardt, reside in similar locations within the laptop as the corresponding software in the ’649 patent and function in a similar manner to that

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

software. And, therefore, when subjected to the same conditions as the software in the '649 patent, a POSITA would understand that the zTrace applications operate and receive notifications in the same way. Limitation 1[g] is thus satisfied.

255. 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 with a security server. *See, e.g.*, Eckardt, 1:35-50 (explaining that there are "programs that the end user must not modify in any way" so those programs are "put in a hidden disk area"), 4:52-59 (explaining that the hard drive partition and its contents "cannot be read or modified"); EX1007 ("zTRACE GOLD is undetectable and unerasable on [the] laptop's hard drive."); EX1013 (zControl is described as an "invisible software application"); EX1026; EX1053; EX1019, 2-3; Kesler, [0009] ("The software is difficult to detect on the computer being traced;" "Because the tracing software [operates] without any prompt or alert, the user (a thief or person in possession of a stolen computer) is unaware of and unable to stop the process."), [0017] (the client software is "installed onto track zero" of the hard drive; "[T]he

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

software will download invisibly and install itself, which significantly reduces the opportunity for tampering”); *see also* my related opinions for limitations 1[e] and 1[f] under **Grounds 1** and **2**. If communications are not protected or concealed, the zTrace™ service would be rendered useless because the unauthorized user of the stolen laptop would become aware of the security software as soon as communication occurred and could delete or disable the communication functionality, rendering the zTrace service inoperable to achieve its intended purpose of allowing laptop owners to recover laptop data and hardware that has been lost or stolen.

256. 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.

VII. NO SECONDARY CONSIDERATIONS OF NONOBVIOUSNESS

257. In the parallel district court litigation, Patent Owner responded to an interrogatory request for information about any potential secondary considerations of nonobviousness for the '649 patent as well as the other six patents in suit, and attempted to assert commercial success, long felt need, failure by others and

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

copying. EX1056 [rog #7], 20-21. Patent Owner, however, did not provide any meaningful evidence, explanation or nexus to specific claim limitations that would support any of these asserted secondary considerations. Only high-level, generic statements were made. I understand from counsel that this is insufficient to show secondary considerations. To the extent Patent Owner supplements this interrogatory or otherwise provides more evidence that such secondary considerations exist, I reserve the right to address that evidence in another declaration.

Declaration of Dr. Polish in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 8,506,649 B2

VIII. CONCLUSION

258. In signing this Declaration, I recognize that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in this proceeding. If required, I will appear for cross-examination at the appropriate time.

259. I hereby declare that all statements made herein of my own knowledge are true and that all statements are made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.

Respectfully submitted,



Dr. Nathaniel Polish

Appendix A

NATHANIEL POLISH, Ph.D.
Daedalus Technology Group, Inc.
350 Seventh Avenue
New York, NY 10001
(212) 684-3890

business experience

2019-present	President, Founder SuperAlert, Inc. SuperAlert has developed a range of wireless sensors used for monitoring building systems in large New York City residential buildings. SuperAlert manufactures, deploys, and operates sensor suites and generates notifications and alerts for building personnel and owners.	NEW YORK, NY
1980-present	President Daedalus Technology Group, Inc. successor to NPS ASSOCIATES Co-founded computer consulting firm. Employs up to twenty people as needed.	NEW YORK, NY
clients include	Intellectual Property Consulting. Various anonymous clients. Consulting on patent valuation and strategy: Act as an advisor on technical and intellectual property matters to various clients. Developed intellectual property for various companies. 2001- present.	NEW YORK, NY
	SpokenHub. Predictive dialer deployment and operation: During the 2012 election cycle assembled and ran a team of engineers to deploy, debug, and operate a large scale outbound calling server farm. This server farm supported hundreds of agents and millions of minutes of calling. 2012.	NEW YORK, NY
	Risk Solutions International. Risk management: Developed technology platform to allow for complex question and answer sessions with airport managers. The results of the sessions then generated planning documents used in risk management. Results were published as part of a Transportation Research Board research program. 2011-2013.	NEW YORK, NY
	Smart Systems/Specialty Acquirer. Advanced Transit fare collection: Founding member of board of directors. Advisor on technical and intellectual property matters. Developed intellectual property for the company. The company is engaged in the development and sale of advanced fare collection systems for mass transit using RFID technologies. 2004-present.	NEW YORK, NY
	Skywi. Wireless broadband: Founding board of directors member. Advisor on technical and intellectual property matters. The company provides a variety of wireless broadband services to semi-rural customers using mesh networks. 2004-2009	FORT WORTH, TX
	Placecorp. Wireless text messaging system: Designed and developed a very large scale, multi-platform text messaging system. Acted as the lead technologist for a startup. In this capacity attended many venture capital meetings and developed all technical sections to the business plans. The system integrated advanced Interactive Voice Response (IVR) with email, paging, and SMS messaging. Oversaw and planned initial development of very small paging device to be manufactured in very high volume. 2000-2001.	NEW YORK, NY
	Marketboy. Distributed market making system: Provided a range of services in the areas of product definition, specification, and implementation strategy. Marketboy was a distributed system that allowed prospective purchasers and vendors to make bid and ask offers for proposed transactions. 2000.	NEW YORK, NY
	Savos. Telephone to streaming audio bridge: Developed, designed and deployed an industrial strength IVR system that allows users to access streaming media via their cell phones. The system supports up to 96 streams on a single chassis. Developed web based content management system and interface for customizable user preferences. 2000.	NEW YORK, NY

deliverENow.

NEW YORK, NY

Online delivery system: Developed a proof of concept prototype of online delivery system. This consisted of a stock clerk server written for Windows CE (Clio) with a CDPD network connection. It demonstrated how purchase and delivery information would be sent to an in-store stock person who prepares them for pickup by a member of the deliverENow courier network. Provided strategic technical advice. Served on board of advisors. Wrote technical specification of business and logistical components of the system. 2000.

Togglethis.

New York, NY

Animation distribution system: Developed critical components of initial version of email-delivered animation system. Components included MacroMedia Director Xtras as well as encryption functions. Developed tools to distribute and manage Togglethis's content, DTG built a custom UNIX email list-server. This server allowed Toggle administrators to create groups, upload episodes, and schedule the delivery of their content. Developed system architecture and language specification for the next version of the IC Engine, which drives the characters. 1998-1999.

JuniorNet.

BOSTON, MA

Children's on-line service: Designed, developed and lead the implementation of a large scale network system for delivery of children's entertainment and education content. Worked with the president and other key players to fit a technology strategy to corporate goals. System is required to serve from 200,000 to 1,000,000 subscribers and be supportable over three to five years. All project goals met within a \$1,000,000+ budget. 1997-2000.

One Click Charge.

NEW YORK, NY

Provide a wide range of consulting services starting with technology evaluation for the principal investor. Provided services in the areas of product definition, team formation and implementation strategy. Developed significant components of a substantial Internet micropayment and authentication system. 1998-2000.

Swatch.

WEEHAWKEN, NJ

Ticketing system: Implemented a radio frequency identification (RFID) based system for providing access to the 1998 Goodwill Games utilizing RFID tagged wristwatches. 1998-1999.

Instant Video Technologies, Inc./Burst.com

SAN FRANCISCO, CA

Burstware --. Designed and developed a series of products to deliver digital video and audio materials over wide-area internet using consumer grade computers. Products were designed to fit within the client's existing patent portfolio. 1995-1997.

Technical evaluation --. Provided technology strategy and evaluation services and acted as Technology Director. 1995-1997.

Assurenent.

BETHESDA, MD

Internet Insurance system --. Designed and developed a system for utilization of the Internet for the distribution and control of insurance agent support software. System can handle tens of thousands of simultaneous users. Member of Board of Directors. 1995-2002.

New Zealand Antarctic Project (NZAP) and US Antarctic Program (USAP).

ANTARCTICA

Penguin Weighbridge -- Designed, developed, and deployed system for tracking the comings and goings, weights, and Ids of Adelie penguins in their natural environment on three colonies on Ross Island, Antarctica. Systems run continuously for months in adverse conditions. System was upgraded and replaced in 2016. 1994-present.

Electronic Digital Documents, Inc.

NEW YORK, NY

Check Image Compression system --. 1995-1999.

American Veterinary Identification Devices, Inc.

NORCO, CA

AVID reader -- Designed and developed digital computer components of radio frequency identification system. Work involved imbedded microcontrollers and real-time digital signal processing in very noisy environment. Designed communications protocols including encryption and error checking schemes. Product in high volume (50,000 unit) production. 1988-1995.

Amprobe Instrument, Inc.

LONG ISLAND, NY

REMCON tester -- Designed and implemented product life-cycle test fixture for a new and innovative solid state switch. Test fixture used by Underwriters Labs for approval. 1988.

Personal Computer Card Corporation

NEW YORK, NY

Smart Cards -- Designed smart card reader/writer system. Performed general design and component selection and wrote software for smart card communications. System design implemented in commercial product. 1987.

The Dun & Bradstreet Corporation

NEW YORK, NY

Voice editing systems -- Designed and built all parts of four generations of interactive voice editing systems. Editing systems produce output used in extensive, high quality speech synthesis system that is part of larger information delivery system. The systems are built on networks of computers in a variety of programming languages and systems. The system involved interactive user interfaces, screen windows, signal processing, and voice file systems. 1982-1991.

1997-2001

Co-Founder, Director and CTO

I-RECALL, INC.

NEW YORK, NY

Co-founded a company that developed software to enable note-taking and linking of notes to streaming media. Used platforms such as PalmPilot and CrossPad for note-taking and provided time-stamped links to audio and video media. Company sold to a focus group company.

1996-1999

Co-Founder, Director, CTO & Principal Product Designer

SOLILOQUY, INC.

NEW YORK, NY

Natural language interfaces to databases: Co-founded in 1996 a company to provide next generation interfaces to structured databases. Developed prototype system using speech recognition and speech synthesis to provide access to music and ecommerce databases. Raised \$1.5 million in angel investments. Company has raised a total of \$8 million through a variety of institutional and individual investors. Hired replacement CTO and exited company in 1999.

1991-1992

President & Principal Product Designer

SIMPLICITY COMPUTING, INC.

NEW YORK, NY

Co-founded in 1991 a computer peripherals manufacturing company concentrating on portable products with international mass-market appeal. Main product: Simplicity Portable Drive, an IBMPC parallel port connected, portable disk storage system. Marketed domestically and in 25+ countries. Products marketed direct via telemarketers, trade shows, sales reps, and national advertising. Products distributed through dealers, distributors and national catalog houses. Company employed 10 people.

- Wrote business plan and raised \$350,000 startup funding
- Established marketing plans
- Directed marketing of products in trade shows, national advertisements and focus groups
- Managed employees
- Designed hardware and software for products
- Supervised hardware & software implementation teams
- First units shipped less than six months from start of project
- Supervised all aspects of manufacturing and testing process
- Contracted with four manufacturing facilities and many suppliers for production
- Supervised and established call-in customer support services

1989-1999

President & CEO

MEASUREMENT & CONTROL PRODUCTS, INC.

NEW YORK, NY

Founded in August 1989 an electronic products development company. M&CP designs, develops, markets and sells its own products through retail, wholesale and catalog channels domestically and abroad. All manufacturing is contracted. Company was profitable in its first year of operation.

Flagship product:

BitView -- Hand held RS-232 data communications diagnostic monitor. Invented, developed and produced hardware and software. Developed and oversaw implementation of marketing strategies, budgets, and business plans. Product currently in third production run.

education

1980-1993

COLUMBIA UNIVERSITY

NEW YORK, NY

Ph.D. in Computer Science, May 1993,

Thesis: *Mixed Distance Measures for the Optimization of Concatenative Vocabularies in Speech Synthesis.*

MPhil in Computer Science, December 1989.

MS in Computer Science, December 1987.

BA in Physics, Columbia College, May 1984.

teaching positions

1997

COLUMBIA UNIVERSITY

NEW YORK, NY

Adjunct Professor, Computer Science.

Advanced undergraduate course: Artificial Intelligence.

1989

COLUMBIA UNIVERSITY

NEW YORK, NY

Graduate Lecturer, Computer Science.

Advanced undergraduate course: Software Design. Taught 68 advanced undergraduates. Supervised two teaching assistants. Students implemented full spreadsheet application under UNIX.

1984-1985

CITY UNIVERSITY OF NEW YORK

NEW YORK, NY

Adjunct Professor, Experimental Psychology.

Graduate-level course: Computer Methods in Experimental Psychology.

publications and patents

2010

Michael L. Beigel, Nathaniel Polish, Steven R. Frank, and Robert E. Malm. Electronic Identification System with Improved Sensitivity. United States Patent 7,737,821B2. June 15, 2010.

2009

Silbernagl, Martin and Polish, Nathaniel. Learning Fare Collection System for Mass Transit. United States Patent 7,568,617. August 4, 2009.

2009

Beigel, Michael L.; Polish, Nathaniel; Frank, Steven R.; Malm, Robert E. Electronic identification system with improved sensitivity. United States Patent 6,472,975. October 29, 2002.

2002

Nathaniel Polish. Bilateral speech system. Speech dialogs for database access. United States Patent 6,430,531. August 6, 2002.

1999

Nathaniel Polish. System and method for distributing and managing digital video information in a video distribution network. United States Patent 5,963,202. October 5, 1999.

1993

Michael L. Beigel, Nathaniel Polish and Robert E. Malm. Multi-Mode Identification System. Fundamental RFID technology. United States Patent 5,235,326. August 10, 1993.

1991

Nathaniel Polish. Mixed Distance Measures for Synthetic Speech Evaluation. In Proceedings of ICASSP-91, Toronto, Canada, 1991.

1988

Nathaniel Polish. A Distributed Signal Processing Facility for Speech Research. In Proceedings of AVIOS88, San Francisco, CA. October 4-6 1988.

1987

Nathaniel Polish. Mixed Distance Measures for Optimizing Concatenative Vocabularies for Speech Synthesis: A Thesis Proposal. Columbia University Department of Computer Science technical report number CUCS-310-87, 1987.

1983

M. Morris, N. Polish, B. Zuckerman, and N. Kaifu. The Temperature of Molecular Gas in the Galactic Center Region. The Astronomical Journal, 88(8):1228-1235, August 1983.

**research
interests**

Computer Speech, Distributed Systems, Interactive Environments. Software Engineering, Systems Engineering, Technology Policy. Knowledge-Based Approaches to Signal Processing. Computational Physics, Non-Linear Dynamics.

**professional
societies**

International Society for Electrical and Electronics Engineers (IEEE), Association of Computing Machinery (ACM), American Association for the Advancement of Science (AAAS).

other interests

Foreign Policy, Political Science, Long Distance Bicycling, United States Space Program.

- grants**
- AT&T Special Projects Grant of \$25,000 for synthetic speech, 1986.
 - Financial support for Ph.D. work was provided by the New York State Science and Technology Foundation Center for Advanced Technology in Computers and Information Systems at Columbia University.
 - Santa Fe Institute Complex Systems Summer School, 2003. Month-long workshop in agent-based models, non-linear systems, and complexity.

1982-present

Technology development projects

Some technology development projects have included:

Wildlife Tracking Systems -- Implemented a remote monitoring system to track and weigh Adelie penguins on Ross Island, Antarctica. System was debugged on-site and made to function in adverse environmental circumstances. 1994-1997, 2016.

Internet Systems -- Implemented a LINUX Internet server with FTP and gopher services. Installed and Internet client for IBM/PC platform. 1994-1995.

Image Compression Technology -- Developed proof-of-concept system for a system to compress images of checks to very small file size. 1994.

Biomedical Systems -- Implemented a large biomedical system used in patient diagnostics. Provided all necessary materials for Food and Drug Administration compliance. 1992-1993.

Synthetic Speech Systems -- Implemented and supported several generations of synthetic speech systems for commercial as well as research purposes. 1985-1999.

Graphics -- Developed high-speed drivers for several graphical devices and evaluated their applicability for interactive uses. Devices included: Vectrix, RAMTEK, Apple Lisa, and IBM Enhanced Graphic Adapter. 1983-1987.

Voice Boards -- Specified function requirements for several generations of high quality voice boards for Q-bus (PDP-11), Apple, MultiBus, and IBMPC bus. Developed high-speed drivers for each of the boards. 1982-1986.

Video Disk and Touch Screens -- Developed experimental interactive system utilizing computer controlled video disks and touch screens. 1982.

1994-present

Intellectual property projects

A separate document detailing intellectual property projects is available on request.

tools

Languages commonly used:

Pascal 1980-1988

C 1985-present.

Other languages used: C++, Lisp, Java and Python .

Assembler:

Intel 8048, 8051, 8088-pentium

Motorola 680xx

TI 320xx signal processors

Zilog Z8, Z80, PIC

Protocols include:

TCP/IP, UDP, RPC and NFS

Operating systems commonly used:

UNIX, MSDOS, Windows and p-system.

In circuit emulators.

Database tools.

ARM processors for embedded systems.

PC bus interfacing.

**contact
information**

polish@dtgroup.com

Office: (212) 684-3890

Academic and business references available upon request.