

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

OpenTV, Inc.,
Patent Owner.

Case No. _____

**DECLARATION OF CHARLES D. KNUTSON, Ph.D.
IN SUPPORT OF APPLE INC.'S PETITION FOR *INTER PARTES*
REVIEW OF U.S. PATENT NO. 5,884,033**

I, Charles D. Knutson, hereby declare as follows:

I. INTRODUCTION

1. I am presently an Emeritus Professor of Computer Science at Brigham Young University in Provo, Utah.

2. I have prepared this Declaration in connection with Apple Inc.'s Petition for *Inter Partes* Review of U.S. Patent No. 5,884,033 (the "033 patent"), which is to be filed concurrently with this Declaration.

3. In the course of preparing this Declaration, I reviewed the '033 Patent, its prosecution file history, as well as the prior art references and related documents discussed in this Declaration, including:

- U.S. Patent No. 5,884,033 ("the '033 Patent") (Apple 1001)
- U.S. Patent No. 5,961,645 ("Baker '645") (Apple 1002)
- U.S. Patent No. 5,696,898 ("Baker '898") (Apple 1003)
- U.S. Provisional App. No. 60/004,670 ("Baker '645 Provisional") (Apple 1004)
- U.S. Patent No. 5,790,554 ("Pitcher '554") (Apple 1005)
- U.S. Patent No. 5,706,507 ("Schloss '507") (Apple 1006)

4. I have been retained by Apple Inc. ("Apple" or "Petitioner") as an expert in the field of computer science, network engineering and architectures, and related technologies. I am being compensated at my normal consulting rate of \$450 per hour

for my time. My compensation is not dependent on and in no way affects the substance of my statements in this Declaration.

5. I have no financial interest in the Petitioner. I similarly have no financial interest in the '033 Patent, the owner of the '033 Patent, and have had no contact with the named inventors of the '033 Patent.

II. QUALIFICATIONS

6. I received B.S. and M.S. degrees in Computer Science from Brigham Young University (1988, 1994) and a Ph.D. degree in Computer Science from Oregon State University (1998).

7. I have been engaged in the software development industry since 1986 in engineering, management, research, and instructional positions.

8. I was employed as a development engineer, test engineer and manager at Novell, Inc. from March 1989 to September 1994 and during that time became very familiar with the theory and operation of data communication systems.

9. I was Vice President of Research and Development for Counterpoint Systems Foundry, Inc. (acquired in 1997 by Extended Systems, Inc., currently a division of OpenSynergy GmbH) from September 1996 to September 1999. My development group created the infrared beaming capability that 3Com Corporation employed in their PalmOS handheld devices. My development group created infrared and

Bluetooth development platforms that have become de facto standards in the embedded/handheld device market worldwide.

10. I was chair of the Test and Interoperability Committee of the Infrared Data Association (IrDA) from February 1998 to October 1999, and a member of the IrDA Architecture Council from February 1998 to April 2008. I was a member of the Infrared Object Exchange (IrOBEX) Working Group from January 2002 to December 2005, helping to define standards for data object exchange in IrDA and Bluetooth.

11. I created industrial coursework on IrDA and Bluetooth technologies for companies engaged in the business of designing and manufacturing short-range wireless protocol products for the embedded device market.

12. I created and presented short courses on wireless data communications at the Embedded Systems Conference, Portable by Design Conference, Wind River Developers Conference, and other industry venues over a nine year period from 1997 to 2005.

13. I have authored or co-authored two books on networking and data communications, 34 academic articles (18 of which involve data communications), six standards documents for the Infrared Data Association, and 43 trade journal and magazine publications (most of which involve data communications).

14. I have served in leadership positions (including Organizing Committee, Technical Program Committee, Panel Moderator, Session Chair, Tutorial Instructor and Reviewer) at academic conferences focused on wireless data communications and mobile computing, including The ACM SIGMOBILE International Conference on Mobile Computing and Networking, The ACM Symposium on Mobile Ad Hoc Networking & Computing, The IEEE GLOBECOM General Symposium, The IEEE International Conference on Computer Communications and Networks, The IEEE Symposium on Ad Hoc Wireless Networks, The IEEE Vehicular Technology Conference Symposium on Integrated Heterogeneous Wireless Networks, The IEEE Wireless Communications and Networking Conference, and The International Telemetering Conference.

15. I have served as a reviewer for academic journals focused on wireless data communications and mobile computing including IEEE Transactions on Information Technology in Biomedicine and IEEE Transactions on Wireless Communications.

16. I was the founder and Director of the Mobile Computing Laboratory in the Computer Science Department of Brigham Young University in Provo, Utah from 2000 to 2008, conducting research in short-range wireless data communications, with emphasis on infrared and Bluetooth data communications.

17. I designed and created a graduate course in wireless data communications in the Computer Science Department at Brigham Young University, and taught this course annually from 2000 to 2005.

18. During my tenure as Director of the BYU Mobile Computing Laboratory, I advised twelve graduate students (11 M.S., one Ph.D.) whose research focused on wireless data communications.

19. During a three year period (2001–2003) the Mobile Computing Lab engaged actively in wireless medical informatics research, yielding two M.S. graduates and several publications.

20. I am currently an Emeritus Professor in the Computer Science Department at Brigham Young University.

21. For further details regarding my employment and academic history, please refer to my curriculum vitae, attached as Apple 1011.

III. RELEVANT LAW

22. I am not an attorney. For the purposes of this Declaration, I have been informed about certain aspects of the law that are relevant to my opinions. My understanding of the law is summarized below.

23. I have been informed and understand that claim construction is a matter of law and that the final claim construction for this proceeding will be determined by the Patent Trial and Appeal Board.

24. I have been informed and understand that a claim of an unexpired patent in an *Inter Partes* Review is to be given the “broadest reasonable construction in light of the specification.” Accordingly, for the purposes of my analysis in this proceeding, I have applied the broadest reasonable construction of the claim terms as they would be understood by one of ordinary skill in the relevant art in light of the specification around the priority date of the ’033 Patent. I understand that this claim construction standard differs from the legal standard used for construing claim terms at a district court litigation, and therefore I reserve the right to revise my opinions relating to claim construction should I be called to testify in a district court litigation involving the ’033 Patent.

25. I have been informed and understand that a claim is indefinite under 35 U.S.C. § 112(2) if it fails to “inform those skilled in the art about the scope of the invention with reasonable certainty.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2129-30 (2014). If a claim uses a term of degree, the claim is indefinite if the specification does not provide some standard for measuring that degree and if one of ordinary skill in the art could not ascertain the scope of the claim from the specification.

26. I have been informed and understand that a patent claim can be considered to have been anticipated—and therefore not patentable—if all of the elements of a claim are found in a single prior art reference.

27. I have been informed and understand that anticipation does not require a prior art reference to expressly disclose each and every claim element using the same terminology as recited by the claims. I understand that a claim is anticipated if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. For example, I understand that a claim limitation is inherently disclosed if it is not explicitly present in the written description of the prior art but would necessarily be embodied or met by the apparatus or method as taught by the prior art. Moreover, I understand that anticipation does not require the prior art to use the same terminology as the patent claims.

28. I have been informed and understand that a patent claim is obvious and therefore invalid if the claimed subject matter, as a whole, would have been obvious to a person of ordinary skill in the art as of the priority date of the patent based on one or more prior art references and/or the knowledge of one of ordinary skill in the art. I understand that an obviousness analysis must consider (1) the scope and content of the prior art, (2) the differences between the claims and the prior art, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations, if any, of non-obviousness (such as unexpected results, commercial success, long-felt but unmet need, failure of other, copying by others, and skepticism of experts).

29. I understand that a conclusion of obviousness may be based upon a combination of prior art references, particularly if the combination of elements does

no more than yield predictable results. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Moreover, I understand that it can be important, though not required, to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in a way the claimed new invention does. I further understand that to determine obviousness the courts look to the interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art.

30. I understand that in determining whether a combination of prior art references renders a claim obvious, it is helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable expectation of success in doing so. I understand, however, that the teaching, suggestion, or motivation to combine inquiry is not required.

IV. CLAIM CONSTRUCTION ANALYSIS

31. I have been asked to opine on the construction of the following claim limitations:

- “filters specifying immediate action” (claims 1, 15, 23)
- “filters specifying deferred action” (claims 1, 15, 23)
- “Internet sites” (Claims 1, 15, 23)

A. “filters specifying immediate action” and “filters specifying deferred action” (claims 1, 15, 23)

32. The terms “filters specifying immediate action” and “filters specifying deferred action” should be interpreted in light of the '033 Patent specification. The '033 Patent defines these terms by contrasting “immediate action” and “deferred action” filters.

For example, the '033 Patent describes immediate action at Apple 1001 at 4:39-55

(emphasis added):

The filtering system detects when the client opens the data stream for a particular port and IP address (step 100), and searches the filter database for matching filters. The system first searches by port number to get the list of filters with IP addresses associated with meta value ANY PORT and also with the particular opened port (step 102). The system then checks for and retrieves any filters that match the particular IP address. The retrieved filters are checked to determine if any require *immediate* action, i.e., if unconditional allowing or blocking is required (steps 104, 106). If such action is required and it is to allow the transmission, the system allows the transmission to proceed normally (step 108). If the immediate action is to block the transmission, the system takes action to block the transmission (step 110), and provides a “Blocked” message to the user (step 112).

33. Thus, “immediate action” is taken when a filter specifies a port number and/or IP address that matches that of the network message. By contrast, a “deferred action” filter requires matching keywords or patterns within the message. For example, at Apple 1001 at 5:8-15, the '033 Patent states:

Deferred filter entries preferably have additional fields, including fields for (1) a keyword, typically a command such as GET; (2) a filter pattern to be compared to data in the message, typically a string of characters; (3) a directional indicator (IN/OUT) for indicating incoming or outgoing transmissions; (4) a compare directive for the type of match;

and (5) an action to be taken, typically to allow or block the transmission.

34. The '033 Patent describes how immediate and deferred action filters operate on a typical message sent over a network. Such a typical message might be an HTTP request for a particular resource sent over port 80 (the standard port for HTTP requests), such as “http://www.domain/test.html,” to use the example provided by the '033 Patent at Apple 1001 at 6:11-12. The “www.domain” portion of the URL is resolved to IP address 1.2.3.4 by querying a DNS (Domain Name Service) server.¹ The '033 Patent then states, “If that IP address and port 80 (or that IP address with ANY PORT) are together in a BLOCK filter, the system prevents the datastream from opening.” Apple 1001 at 6:16-18. But “[r]ather than specifying blocking at this time,” the '033 Patent states, “a filter can indicate a deferred action.” *Id.* at 6:19-20. For example, the deferred filter can search for the pattern “test.html,” and if there is a deferred filter matching that pattern, the system can block it. *Id.* at 6:20-28.

35. While the words “immediate” and “deferred” suggest a temporal relationship between the two filter types, the claim language shows that the patentee did not intend any such relationship. Element (c) of claim 1 recites, “comparing information in the message to filtering information in at least one of said filters specifying

¹ The example in the '033 specification, “www.domain,” is not actually a valid Internet domain because it is missing an extension, such as “.com” or “.org.”

immediate action and said filters specifying deferred action.” Thus, if a message were compared only to a deferred filter, it would meet this limitation. There is no requirement in claim 1 that a message must first be compared with an immediate filter, and then, if there is no match, compared with a deferred filter. Rather, as the claim language makes clear, immediate and deferred filters are two different types of filters, at least one of which is compared with the message, in no particular time order.

36. During prosecution, the patentee attempted to overcome the Shewd reference by arguing that the claimed filters operate “between the presentation and application levels (layers 6 and 7, respectively) of the seven-level ISO protocol model.”² Apple 1007.064. This argument has no basis in the specification, and the patentee did not amend the claims to add such a limitation. In fact, this argument is directly contradicted by claims 3 and 4, which depend from claim 1. Claim 3 requires “filters specifying immediate action” to include fields specifying “an interface port” and “an Internet Protocol (IP) address.” And claim 4 further limits claim 3 to require that the step of “comparing information in the message to filtering information” further

² The patentee’s reference to ISO as a “protocol model” is incorrect. ISO is the International Standards Organization, established in 1947. In the 1970s, ISO introduced a networking model called the Open Systems Interconnection (OSI) model, consisting of 7 protocol layers (not “levels”). For the purposes of my analysis, I assume that when the patentee refers to “ISO,” they in fact mean “OSI.”

includes “comparing an Internet Protocol (IP) address.” Internet Protocol (IP) addresses are commonly understood to correspond with layer 3 (network layer) of the seven-layer OSI protocol model and not with layer 6 (presentation layer) or 7 (application layer).³ Rather, claims 3 and 4 are consistent with my construction of “filters specifying immediate action” because a filter specifying a port or network address is broad enough to include a filter specifying both a port and an IP address, as it is narrowed in claims 3 and 4.

37. Thus, the '033 Patent makes it clear that “immediate action” filters operate on the network address or port number, while “deferred action” filters operate by looking for matching keywords or patterns in other portions of the message. One of ordinary skill at the time reading the '033 Patent would therefore have interpreted “filters specifying immediate action” to mean “filters specifying whether the transmission of the message should be unconditionally allowed or blocked based on a port number or network address specified by the message.” Similarly, such a person would have interpreted “filters specifying deferred action” to mean “filters specifying

³ While there are different conventions in the art for enumerating the “layers” of the TCP/IP protocol stack, there is clear consensus in all relevant literature of which I am aware that IP (and its accompanying addressing scheme) is part of the network layer (one of the lower layers in the TCP/IP protocol stack) and not part of a higher protocol layer (such as application or presentation layers).

whether the transmission of the message should be allowed or blocked based on information in the message other than the port number and network address.”

B. “Internet sites” (claims 1, 15, 23)

38. The term “Internet sites” is generally understood in the field of computer networking to refer to a resource that a user can access using the Internet. The Internet is a collection of networks over which messages may be sent using a protocol known as Transmission Control Protocol/Internet Protocol, or TCP/IP. Each “site” on the Internet can be accessed using a network protocol within the TCP/IP suite, such as HTTP or FTP. Thus, one of ordinary skill would understand this term of art to mean “resources accessible on the Internet using TCP/IP.”

39. The ’033 Patent specification is consistent with this understanding. The specification is directed to a system for applying filters to block or allow messages transmitted over the Internet and states at Apple 1001 at 2:41-50:

Messages are transmitted over the Internet among computers with a transport protocol known as Transmission Control Protocol/Internet Protocol (TCP/IP). This protocol provides an error-free data connection between computers and sits underneath and works in conjunction with higher level network protocols, including HyperText Transfer Protocol (HTTP); File Transfer Protocol (FTP); Network News Transmission Protocol (NNTP); Internet Relay Chat (IRC); and GOPHER.

40. Each of these network protocols listed is a protocol by which messages can be sent and received using TCP/IP. The '033 Patent's use of the term "Internet sites" is thus consistent with how one of ordinary skill would understand this term, namely, that it means "resources accessible on the Internet using TCP/IP."

V. LEVEL OF ORDINARY SKILL IN THE ART

41. Based on my review of the '033 patent and my background and experience in the field of computer science, it is my opinion that one of ordinary skill in the art at the time the '033 patent was filed would be someone with a bachelor's degree or higher in computer science, computer engineering, or the equivalent, plus two or more years of experience in the field of networking and data communications, or a similar field.

VI. PRIOR ART

42. I have been asked to compare the following prior art references to claims 1, 2, 9, 15, and 23 of the '033 Patent:

- U.S. Patent No. 5,961,645 ("Baker '645") and U.S. Provisional App. No. 60/004,670 ("Baker '645 Provisional")
- U.S. Patent No. 5,696,898 ("Baker '898")
- U.S. Patent No. 5,790,554 ("Pitcher '554")
- U.S. Patent No. 5,706,507 ("Schloss '507")

A. Overview Of Baker '645

43. I understand that Baker '645 was filed on October 1, 1996 and claims priority to Baker '645 Provisional, which was filed on October 2, 1995. I understand that Baker '645 is entitled to the October 2, 1995 priority date to the extent the relevant disclosure in Baker '645 is supported by disclosure in the provisional application. I have reviewed Baker '645 and the provisional application. The material I have relied on from Baker '645 to show that the '033 patent is invalid is supported in the provisional application. I have highlighted specific support in the provisional application in the context of the claim limitations I discuss below.

44. Baker '645 is directed to the same problem addressed by the '033 patent: providing filters to deny or allow access to resources available on the Internet. In Figure 1, Baker '645 discloses a database of filters (115) residing on a proxy server (112) which maintains lists of URLs to which each user terminal (107-109) has access. Apple 1002 at 4:1-16. Baker defines a filter at Apple 1002 at 1:29-33 as follows: "A program that controls access to remote resources will be termed a filter. A filter may be embodied in software running on the client machine or on a separate machine."

B. Claim 1 Of The '033 Patent Is Anticipated By Baker '645

45. It is my opinion that Baker '645 anticipates claim 1 of the '033 patent. I discuss each limitation below.

1. Preamble: A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:

46. Baker '645 is directed to filters implemented on a computer for controlling access to Internet sites. For example, at Apple 1002 at 1:12-25, Baker '645 discloses:

The invention relates to controlling database access and, more particularly, to selectively providing such control with respect to otherwise public databases which include naming ambiguities for their resources. . . . The collection of all such publicly available resources, linked together using files written in Hypertext Mark-up Language ('HTML'), and including other types of files as well, is known as the World Wide Web ('WWW').

47. This disclosure is supported by the provisional application at the first paragraph of page 1, which states, "[a] number of systems and methods have been proposed or created to control access to remote resources publicly available to users of other computers through the collection of networks known as the Internet. The collection of all such publicly available resources, linked together using files written in Hypertext Mark-up Language ('HTML'), is known as the World Wide Web ('WWW')." Apple 1004 at 1.

2. "(a) opening a data stream to send a message through an interface to an Internet server"

48. The '033 patent describes a system for restricting access to Internet resources. One of ordinary skill in the art would have been familiar with TCP/IP protocols and would have known that initiating any network communication using TCP/IP

protocols would necessarily require “opening a data stream to send a message through an interface to an Internet server.” This limitation is therefore inherently disclosed by any reference describing TCP/IP communications. Baker ’645 discloses this limitation at Apple 1002 at 1:48-53 because it discloses sending messages by HTTP, which is a TCP/IP protocol: “Resources are requested in the Hypertext Transport Protocol (‘http’) by means of a name such as a Uniform Resource Identifier (‘URI’) referring to a resource at the destination machine, or a Uniform Resource Locator (‘URL’) which contains both a URI and the domain name or IP address of the remote site which the URI is stored.” This disclosure is supported at page 3 of the provisional application, which discusses requesting responses from remote servers using a URL. Apple 1004 at 3.

49. In addition, the ’033 patent admits that opening a data stream is an inherent part of sending a message using TCP/IP. For example, describing the “current version,” (version 4) of Internet Protocol, the ’033 patent states at Apple 1001 at 2:58-60, “[t]o initiate communications with another computer over the Internet, a computer opens a port in its interface for a TCP data stream.”

3. “(b) maintaining a database of filtering information comprising a table of filters, said table comprising”

50. Baker ’645, at Apple 1002 at 4:11-21, discloses a database of filters including a list of URLs each terminal has permission to access:

The processor 111 is coupled to a database 115. The database 115 stores information about the network resources 101-105, in the form of URLs, and the user terminals 107-109 in the form of terminal IDs. The processor 111 can query the database 115 before allowing a terminal to receive a particular URL. For example, the database 115 may store a list of URLs that each user terminal 107-109 has permission to access. In this example, the processor 111 will not allow a user terminal 107-109 to receive a URL that it does not have permission to receive.

51. This disclosure is supported at pages 3 and 4 of the provisional application, which describes “look[ing] up any or all of these URLs in the database to determine whether to provide the final resource to the client,” and that “the filter can look up the new URL in the ratings database to determine whether to allow the resource or forbid it to the client.” Apple 1004 at 3-4.

4. “(1) filters specifying immediate action, and”

52. Baker '645 discloses immediate action filters, which specify whether to allow access to a particular network address: “The processor 111 can query the database 115 before allowing a terminal to receive a particular URL. For example, the database 115 may store a list of URLs that each user terminal 107-109 has permission to access. In this example, the processor 111 will not allow a user terminal 107-109 to receive a URL that it does not have permission to receive.” Apple 1002 at 4:14-21. This is

supported at pages 3 and 4 of the provisional application, as I discussed immediately above. Apple 1004 at 3-4.

5. “(2) filters specifying deferred action;”

53. Baker '645 provides several examples of deferred action filters. First, filtering may be performed on the basis of a content rating. In other words, data indicating a rating value must be compared to ratings included in a list of permissible ratings, requiring that the filter match other data besides just network address or port. For example, at 1002 at 4:21-27, Baker '645 discloses “As another example, the database 115 may store a list of ratings corresponding to the URLs, and a list of categories of ratings that each user terminal 107-109 is allowed receive. In this example, the processor 111 will not allow a user terminal 107-109 to receive a URL that has a rating that is not included in that terminal's category of permissible ratings.” This disclosure is supported at page 4 of the provisional application, which states, “A second way of using response information is to make it possible for the filter to access ratings in the ratings database based on a checksum computed from a response resource.” Apple 1004 at 4.

54. Second, Baker '645 discloses at Apple 1002 at 5:26-30 that “[t]he above schemes can be used separately or in combination. They can also be used in other situations in which naming problems arise, such as in systems using databases of keywords in resources, annotations of resources, quality ratings, or categorizations of

resources.” Thus, “databases of keywords in resources” can also be used to allow or forbid access to Internet resources. This is another example of a deferred filter, and Baker ’645 states that this scheme can be used “in combination” with the other filters (e.g., immediate filters) disclosed above. This same statement is repeated at page 4 of the provisional application. Apple 1004 at 4.

55. Third, the provisional application also states, at Apple 1004 at 3, “When the filter receives a request for a URL, rather than deciding immediately whether to allow or deny the resource, the filter may choose to request the resource and make a decision based on the response. This decision may be based on the response header or on the response resource.” Baker ’645 discloses similar material at Apple 1002 at 3:24-35. Since the decision to allow or forbid access is not based on the original URL but rather by matching patterns in data returned in the response, this is another example of a deferred filter.

6. “(c) comparing information in the message to filtering information in at least one of said filters specifying immediate action and said filters specifying deferred action; and”

56. Baker ’645 discloses that a request for a resource is compared with the filter information at Apple 1002 at 4:16-27: “For example, the database 115 may store a list of URLs that each user terminal 107-109 has permission to access. . . . In this example, the processor 111 will not allow a user terminal 107-109 to receive a URL that has a rating that is not included in that terminal's category of permissible ratings.”

This is supported at least at pages 3 and 4 of the provisional application, as described above at paragraph 51. Apple 1004 at 3-4.

7. “(d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.”

57. The same disclosure I relied upon immediately above illustrates that Baker ’645 compares a requested URL to information in the filter database to determine whether to allow transmission of the outgoing message. Apple 1002 at 4:16-27; Apple 1004 at 3-4. In addition, Claim 6 of Baker ’645 recites, in part:

A public network resource access system . . . wherein said processor is programmed to: a) receive a request for at least one of said plurality of network resources from a user, said request including a first resource identifier and a user identification code; b) determine whether to submit said first resource identifier to said network by querying a database using said first resource identifier and said user identification code. . .

58. In other words, the “first resource identifier” in the message is compared to information retrieved by “querying a database” to determine whether to submit the request to the network. This is supported at least at page 3 of the provisional application, which states that the filter may “look up any or all of these URLs in the database to determine whether to provide the final resource to the client.” Apple 1004 at 3.

59. Based on the analysis above, it is my opinion that Baker '645 anticipates claim 1 of the '033 patent.

C. Claim 2 Of The '033 Patent Is Anticipated By Baker '645

60. It is my opinion that Baker '645 anticipates claim 2 of the '033 patent, as I discuss in detail below.

1. “2. The method of claim 1, wherein some of the filters indicate that the message should be sent, and others indicate that the message should be blocked.”

61. Baker '645 discloses that some filters specify ratings that are permissible and others that are not, thus indicating that requests for some resources should be sent while others should be blocked. For example, Baker '645 discloses the following at Apple 1002 at 4:14-27:

The processor 111 can query the database 115 before allowing a terminal to receive a particular URL. For example, the database 115 may store a list of URLs that each user terminal 107-109 has permission to access. In this example, the processor 111 will not allow a user terminal 107-109 to receive a URL that it does not have permission to receive. As another example, the database 115 may store a list of ratings corresponding to the URLs, and a list of categories of ratings that each user terminal 107-109 is allowed receive. In this example, the processor 111 will not allow a user terminal 107-109 to receive a URL that has a rating that is not included in that terminal's category of permissible ratings.

62. This disclosure is supported in the provisional application at pages 3 and 4.

Apple 1004 at 3-4. Thus, it is my opinion that Baker '645 also anticipates claim 2.

D. Claim 9 Of The '033 Patent Is Anticipated By Baker '645

63. It is my opinion that Baker '645 anticipates claim 9 of the '033 patent, as I discuss in detail below.

1. **“9. The method of claim 1, wherein steps (a)-(d) are all performed by a client computer, step (b) including maintaining the database in storage residing on the client computer.”**

64. Baker '645 discloses that the filtering operations and database may be located on the client itself or on a separate server as a matter of design choice. For example, at Apple 1002 at 1:29-32, Baker '645 states, “A program that controls access to remote resources will be termed a filter. A filter may be embodied in software running on the client machine or on a separate machine.”

65. Baker '645 further discloses the following at Apple 1002 at 3:53-67:

FIG. 1 is a simplified diagram of an embodiment of a system that can utilize the present invention. As shown in FIG. 1, the system includes a public network 100, network resources 101-105, and a user site 106. Particular users at the user site 106 gain access to the public network 100 via user terminals 107, 108 and 109. Each of the user terminals 107-109 is linked by a local area network (“LAN”) 110 to a processor 111 within a proxy server 112. Proxy server 112 provides a connection from the processor 111 to the public network 100 via a firewall 113. In the embodiment shown in

FIG. 1, the processor 111 runs filtering code which controls access to the network resources 101-105 by the user terminals 107-109.

However, each user terminal 107-109 can also include a processor that runs filtering code for individually controlling access for each terminal.

66. Thus, in Figure 1, the processor running the filtering code resides on a proxy server. But Baker '645 discloses that each terminal, which are the clients running a web browser, can also include a processor that runs the filtering code. This is an example of a trade-off between using a thin client and a thick client, which was well known to those of ordinary skill in the art at the time the '033 patent was filed. A thin client refers to simplified terminal software that does not need a powerful processor or a large amount of storage because most of the processing is pushed off to other systems on the network. A thick client, on the other hand, generally requires more processing power and more local storage and can take care of more tasks on its own, without relying on other resources on the network. Baker '645 simply expresses this trade off by noting that the filtering can be pushed off to other servers on the network (thin client model) or performed on the client itself (thick client model). Thus, Baker '645 also anticipates claim 9 of the '033 patent.

E. Claims 15 And 23 Of The '033 Patent Are Anticipated By Baker '645

67. It is my opinion that Baker '645 anticipates claims 15 and 23 of the '033 patent. While claim 1 is directed at network messages that are sent from the client to the

Internet resource, claim 23 is directed to messages arriving at the client from the Internet resource, and claim 15 does not specify the direction of the message. In other respects, these claims have essentially the same scope.

68. It is my opinion that Baker '645 anticipates claims 15 and 23 for the same reasons it anticipates claim 1 because it discloses that the filtering operations may be performed on either outgoing (client to server) or incoming (server to client) messages. For example, Baker '645 discloses the following at Apple 1002 at 3:24-35:

One approach is to consider responses from remote servers as well as requested URLs in determining whether to allow or deny resources. The response information used may include header information or the resource itself. If the header information includes a new URL, the new URL can be forwarded to the requestor, or submitted to the public network. A permission database is queried to determine whether a resource corresponding to the new URL should be forwarded to the requestor.

69. This passage indicates that the filters may consider “requested URLs,” which are outgoing messages requesting access to a resource, as well as “responses from remote servers,” which are messages arriving from servers, thus disclosing operation on both outgoing and incoming messages. The URL filters, as described above, may be applied to the original (outgoing) request, or to new URLs returned by remote servers, which would be incoming messages. This concept is supported in the provisional application at least at Apple 1004 at 3, which states, “[o]ur invention uses

two approaches to handle naming ambiguities in a filter. One is to consider responses from remote servers as well as request URLs in determining whether to allow or deny resources.” Thus, it is my opinion that Baker ’645 also anticipates claims 15 and 23 for the same reasons it anticipates claim 1.

F. Overview Of Baker ’898

70. I understand that Baker ’898 (Apple 1003) was filed on June 6, 1995 and qualifies as prior art to the ’033 patent. I have reviewed Baker ’898, and it is my opinion that it anticipates claims 1, 2, and 15 of the ’033 patent and renders claims 9 and 23 obvious in view of the knowledge of one of ordinary skill in the art. It is also my opinion that the combination of Baker ’898 and Baker ’645 render claims 9 and 23 obvious.

71. Baker ’898 discloses a database of filters to control access to Internet sites. For example, at Apple 1003 at 3:4-16, Baker ’898 discloses filters implemented on a proxy server within the user’s local network for controlling access to Internet resources:

The invention employs a relational database to determine access rights, and this database may be readily updated and modified by an administrator. Within this relational database specific resource identifiers (i.e., URLs) are classified as being in a particular access group. The relational database is arranged so that for each user of the system a request for a particular resource will only be passed on from the local network to a server providing a link to the public/uncontrolled database if the resource identifier is in an

access group for which the user has been assigned specific permissions by an administrator. The invention is implemented as part of a proxy server within the user's local network.

72. The filters disclosed in Baker '898 may list URLs that should be allowed or URLs that should be blocked, as disclosed at Apple 1003 at 4:27-34:

In the particular embodiment described above, relational database 114 stores a list of user terminal identification codes and the various URLs that each user terminal should be allowed to transmit to public network 100. It will be understood that the invention could be modified so that the list of associated URLs associated with a given user terminal identification code serves as a list of URLs that that particular user terminal is not permitted to contact.

73. These lists of network addresses that can be blocked or allowed are “filters specifying immediate action,” as claimed in the '033 patent. Baker '898 also discloses “filters specifying deferred action” in the context of the '033 patent because it teaches that filters may also be specified to match particular patterns or keywords in a URL request. For example, at Apple 1003 at 5:39-47, Baker '898 discloses the following:

In order to specify that students be allowed to view “history” resources, but excluded from “history answer” resources, the relational database would store the following with expression rules that would be associated with student identification codes:

+http://ourschool.edu/history/*

-http://ourschool.edu/history/*answer*

The notation “+” indicates a grant of access to a resource, and the “-” indicates a restriction.

74. Baker ’898 explains that these filter entries are “regular expressions . . . typical of UNIX shell languages,” which can be used for pattern matching, with the “*” character matching any string of symbols. Apple 1003 at 5:26-36. Such filters match keywords or phrases in the full URL request to determine access permissions. These filters are thus “deferred” action filters in the context of the ’033 patent. A detailed explanation of my opinion that Baker anticipates claims 1, 2, and 15 follows.

G. Claim 1 Of The ’033 Patent Is Anticipated By Baker ’898

1. Preamble: A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:

75. Baker ’898 is directed to filters implemented on a computer for controlling access to Internet sites. For example, the Abstract of Baker ’898 discloses:

A system and method for selectively controlling database access by providing a system and method that allows a network administrator or manager to restrict specific system users from accessing information from certain public or otherwise uncontrolled databases (i.e., the WWW and the Internet). The invention employs a relational database to determine access rights, and this database may be readily updated and modified by an administrator.

2. “(a) opening a data stream to send a message through an interface to an Internet server”

76. As I explained in my discussion of the Baker '645 reference, this limitation is inherently disclosed by any reference describing TCP/IP communications. Baker '898 discloses this limitation at Apple 1003 at 1:17-30 because it discloses requesting resources on the World Wide Web using HTTP, FTP, and Gopher, each of which are TCP/IP protocols.

3. “(b) maintaining a database of filtering information comprising a table of filters, said table comprising”

77. Baker '898, at Apple 1003 at 3:4-14, discloses a relational database of filters including a list of URLs each terminal has permission to access:

The invention employs a relational database to determine access rights, and this database may be readily updated and modified by an administrator. Within this relational database specific resource identifiers (i.e., URLs) are classified as being in a particular access group. The relational database is arranged so that for each user of the system a request for a particular resource will only be passed on from the local network to a server providing a link to the public/uncontrolled database if the resource identifier is in an access group for which the user has been assigned specific permissions by an administrator.

78. These resource identifiers, organized into access classes, comprise a table of filters within the relational database.

4. “(1) filters specifying immediate action, and”

79. Baker '898, at Apple 1003 at 4:11-20, discloses immediate action filters, which specify whether to allow access to a particular resource based on the network address: “For example, upon receipt of a URL from user terminal 107 requesting information from network resource 102, processor 111 would access relational database 114, and thereby determine that URL102 was indeed an allowable request. Following this determination, processor 111 would forward URL102 to public network 100 via firewall 113. Contrastingly, if a URL that is not associated with the requesting terminal identification code within relational database 114 is received by processor 111, that request for information is denied.”

5. “(2) filters specifying deferred action;”

80. Baker '898 discloses that the table also includes deferred action filters, which do not unconditionally block a particular Internet site but rather search for particular keywords or patterns, in resource names, which, if found, cause the resource to be blocked or allowed. For example, at Apple 1003 at 5:30-47, Baker '898 discloses:

In this case, a notation for regular expressions is employed that is typical of UNIX shell languages, wherein “*” represents any string of symbols, including the empty string. The URL `http://ourschool.edu/subject/*answer*` specifies any resources within the directory `http://ourschool.edu/subject` (or its tree of subdirectories) that contain “answer” in their names. Access to the “answer” resources would most likely be restricted to instructors

(i.e., students would not be able to view the answers). In order to specify that students be allowed to view “history” resources, but excluded from “history answer” resources, the relational database would store the following with expression rules that would be associated with student identification codes:

+http://ourschool.edu/history/*

-http://ourschool.edu/history/*answer*

The notation “+” indicates a grant of access to a resource, and the “-” indicates a restriction.

81. Baker ’898 also discloses, at Apple 1003 at 2:33-37, that “[i]n still another method of ‘filtered’ access to WWW resources, the client or proxy server checks each resource for a list of disallowed words (i.e., obscenities; sexual terms, etc.) and shows the user only those resources that are free of these words.” This method of filtering matches specific disallowed words in network messages and selectively blocks messages containing those words. This is also a form of “deferred” filter in the context of the ’033 patent.

6. “(c) comparing information in the message to filtering information in at least one of said filters specifying immediate action and said filters specifying deferred action; and”

82. The regular expression matching I discussed above that is disclosed in Baker ’898 discloses comparing information in the message to filtering information in the database. For example, comparing the URL request message to the filter “http://ourschool.edu/history/*” allows matching resources (due to the “+”) and

matching the URL request message to “http://ourschool.edu/history/*answer*”

blocks matching requests (due to the “-”). *See* Apple 1003 at 5:30-47.

7. (d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.

83. Baker '898 discloses that the results of the comparison I discussed above are used to block or allow the network message: “The notation ‘+’ indicates a grant of access to a resource, and the ‘-’ indicates a restriction.” Apple 1003 at 5:46-47. Baker '898 also discloses, at Apple 1003 at 4:11-20, with respect to the “immediate” filters, that messages requesting URLs that match those listed in the database of allowed sites are allowed: “For example, upon receipt of a URL from user terminal 107 requesting information from network resource 102, processor 111 would access relational database 114, and thereby determine that URL₁₀₂ was indeed an allowable request. Following this determination, processor 111 would forward URL₁₀₂ to public network 100 via firewall 113. Contrastingly, if a URL that is not associated with the requesting terminal identification code within relational database 114 is received by processor 111, that request for information is denied.”

84. Based on the analysis above, it is my opinion that Baker '898 anticipates claim 1 of the '033 patent.

H. Claim 2 Of The '033 Patent Is Anticipated By Baker '898

85. It is my opinion that Baker '898 anticipates claim 2 of the '033 patent, as I discuss in detail below.

1. “2. The method of claim 1, wherein some of the filters indicate that the message should be sent, and others indicate that the message should be blocked.”

86. Baker '898 discloses a specific example of a filter that allows access to “history” resources and another that blocks access to “answer” resources by allowing or blocking requests that match certain patterns in the requested URL. The filter that “indicates the message should be sent” is indicated using a “+,” while the filter that indicates a message should be blocked is indicated using a “-.” This is disclosed at Apple 1003 at 5:39-47:

In order to specify that students be allowed to view “history” resources, but excluded from “history answer” resources, the relational database would store the following with expression rules that would be associated with student identification codes:

+http://ourschool.edu/history/*

-http://ourschool.edu/history/*answer*

The notation “+” indicates a grant of access to a resource, and the “-” indicates a restriction.

87. Thus, it is my opinion that Baker '898 also anticipates claim 2.

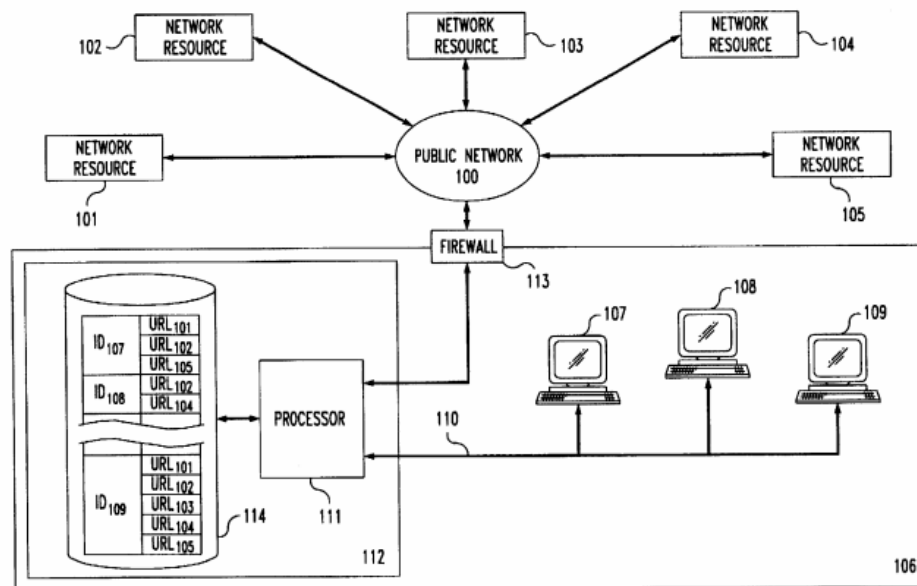
I. Claim 15 Of The '033 Patent Is Anticipated By Baker '898

88. While claim 1 is directed at network messages that are sent from the client to the Internet resource, claim 15 does not specify the direction of the message and is thus broader than claim 1. Therefore, it is my opinion that Baker '898 anticipates claim 15 for the same reasons it anticipates claim 1.

J. Claim 9 Of The '033 Patent Is Rendered Obvious By Baker '898 Alone Or In Combination With Baker '645

1. “9. The method of claim 1, wherein steps (a)-(d) are all performed by a client computer, step (b) including maintaining the database in storage residing on the client computer. ”

89. Baker '898 discloses a database of filters that is maintained on a proxy server, as shown in Figure 1, which is reproduced below:



90. The database, element 114, includes sets of filters, each associated with a particular terminal. For example, the set labeled ID₁₀₇ in database 114 includes three URLs—URL₁₀₁, URL₁₀₂, and URL₁₀₅—each associated with terminal 107. Because the filters are already divided up to be specific to individual terminals, it would have been an obvious design choice to implement the filter database on the individual terminals, or clients, and to process the filtering algorithms on the processors in the terminal clients rather than on the processor 111 in the proxy server. Doing so would simply

mean adopting a thick client framework instead of the thin client framework shown in Figure 1. It was well known at the time the '033 patent was filed that networks could be designed to use thin clients, with relatively little processing power and storage at the individual clients, or thick clients, where more computing power and storage was implemented in the client computers. Thus, storing filter parameters and processing the filtering algorithm on the client computers themselves would have been a matter of design choice and one that those of ordinary skill in the field of computer science or computer networking would have expected to be successful. It is therefore my opinion that Baker '898, in combination with the knowledge of one of ordinary skill in the art, renders claim 9 obvious.

91. Alternatively, one of ordinary skill would have been motivated to combine Baker '898 with Baker '645. These two references share a common inventor, and Baker '645 includes an explicit reference to Baker '898, which would have motivated one to look at the references together: Baker '645 states, "A filter may be embodied in software running on the client machine or on a separate machine. In one embodiment, the database or permissions derived from the database are stored local to filter, either on the same machine or within a common firewall. Such a system is described in U.S. patent application Ser. No. 08/469,342, 'System and Method for Database Access Control,' filed on Jun. 6, 1995." Apple 1002 at 1:32-39. The referenced application number is the application that issued as Baker '898. Thus,

Baker '645 instructs the reader to look to Baker '898 and does so in the context of pointing out that the filter may be embodied either on the client itself or on a separate proxy server. This explicit suggestion in Baker '645 to implement the system of Baker '898 on the client thus motivates the combination and renders claim 9 of the '033 patent obvious.

K. Claim 23 Of The '033 Patent Is Rendered Obvious By Baker '898 Alone Or In Combination With Baker '645

92. Claim 23 of the '033 patent is essentially commensurate in scope with claim 1 except that claim 1 is directed to outgoing (client to server) messages while claim 23 is directed to incoming (server to client) messages. As I discussed above, Baker '898 is primarily directed to blocking or allowing outgoing URL requests. However, Baker '898 points out that sometimes, when a request for a URL is sent out, the server may return a response that includes new URLs pointing to other Internet resources. For example, at Apple 1003 at 1:27-30, Baker '898 states “[w]hen a resource is downloaded, it may include the URLs of additional resources. Thus, the user of the client can easily learn of the existence of new resources that he or she had not specifically requested.” It would have been obvious to one of ordinary skill that a filter would not be completely effective if a request for a URL were allowed by the filter but if the server that was accessed then returned a new URL that might direct the browser elsewhere to content that might be offensive. It would have been obvious, then, to apply the same filters to the *incoming* message returned by the

server to make sure that the redirected URL was also one that was allowed, or to block the message if the new returned URL were one that should be blocked.

Therefore, it would have been obvious to apply the filter database also to incoming messages. Baker '898, in light of the knowledge of one of ordinary skill, thus renders claim 23 obvious.

93. Alternatively, it would have been obvious to combine the teachings of Baker '898 with those of Baker '645. Again, because the two references share an inventor, because of the explicit reference to Baker '898 in Baker '645, and because they are directed to the same subject matter, one of ordinary skill would have been motivated to look to the teachings of the two references together. Further, as I discussed above, Baker '898 specifically mentions the problem of new URLs returned by a server on the Internet. Baker '645 specifically teaches methods of dealing with URL redirections and URLs returned by Internet servers. Baker '645 states, at Apple 1002 at 5:1-4, "On the other hand, if the response is a resource with a field specifying a new URL, the processor 111 can look up the new URL in the database 115 to determine whether to allow the resource or forbid it to the requesting terminal." Thus, it explicitly teaches that the *incoming* response can be compared to the filter database to determine whether the message should be allowed or blocked. Thus, the combination of Baker '898 and Baker '645 renders claim 23 obvious.

L. Overview of Pitcher '554

94. I understand that Pitcher '554 (Apple 1005) was filed on October 4, 1995 and qualifies as prior art to the '033 patent. I have reviewed Pitcher '554, and it is my opinion that it anticipates claims 1, 2, 15, and 23 of the '033 patent and renders claim 9 obvious in view of the knowledge of one of ordinary skill in the art. It is also my opinion that the combination of Pitcher '554 and Baker '645 renders claim 9 obvious.

95. Pitcher '554 discloses a system for filtering messages sent over the Internet and can filter based on (1) network address information, or (2) “content of the data packets.” Apple 1005 at 3:52-53. An embodiment of the system disclosed in Pitcher '554 operates on a LAN switch used to facilitate internetworking: “LAN switches enlarge router subnets, flatten the internetwork, simplify management, and reduce the cost of internetworking.” Apple 1005 at 2:52-55. The Internet is an example of internetworking. Pitcher '554 states that an “embodiment of the present invention defines a pattern and performs a forwarding action specified for packets whose contents match or do not match the pattern.” Apple 1005 at 3:53-56. Such filters that match patterns in the message are “deferred” filters in the context of the '033 patent. Pitcher '554 also discloses filters that either forward (allow) or drop (block) messages based on their destination address. For example, Pitcher presents an example of “FLTR_002,” which is a single-stage filter that performs an action on any message directed to MAC address “00.80.00.02.31.54.” Apple 1005 at 7:12-15. It was

well known to those of ordinary skill at the time the '033 patent was filed that a MAC address is an address identifying a particular device on a network which either sends a message or is the intended recipient of a message. Thus, FLTR_002 is an immediate action filter in the context of the '033 patent, which blocks or allows a message based on its network address.

96. A detailed explanation of my opinion that Pitcher '554 anticipates claims 1, 2, 15, and 23 follows:

M. Claim 1 Of The '033 Patent Is Anticipated By Pitcher '554

1. Preamble: A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:

97. Pitcher '554 is directed to filters implemented within a computer network to control access to Internet sites. Pitcher '554 discloses, at Apple 1005 at 3:48-53, the following:

The present invention relates to the field of data networking. Specifically, the present invention relates to a method and apparatus for filtering, i.e., controlling the forwarding of, data packets from a network device, such as a LAN switch, onto a network coupled thereto based on the content of the data packets.

The system of Pitcher '554 is designed to work in an internetworking environment, an example of which is the Internet. *See* Apple 1005 at 2:52-55. Specifically, it operates in a client-server environment to filter messages to or from internetworked servers.

“High powered workstations and servers may be connected directly to the LAN

switch . . .”, Apple 1005 at 2:49-50, and filters may be implemented on the LAN switch. *See* Apple 1005 at 3:48-53. Pitcher ’554 thus discloses communicating with servers over networks such as the Internet to prevent or allow access.

2. “(a) opening a data stream to send a message through an interface to an Internet server”

98. As I explained in my discussion of the Baker ’645 reference, this limitation is inherently disclosed by any reference describing TCP/IP communications. Pitcher ’554 discloses this limitation at least at Apple 1005 at 6:1-7, because it discloses sending messages using TCP/IP protocols: “Network interface card 526, in conjunction with appropriate data communications protocols (e.g., the TCP/IP suite of internetworking protocols), provide the means by which a network management system operating on computer system 500 exchanges information with other devices coupled to the same computer network such as LAN switch 100.”

3. “(b) maintaining a database of filtering information comprising a table of filters, said table comprising”

99. Pitcher ’554 discloses maintaining a database including a table of filters. Figure 2 of Apple 1005, reproduced below, provides an example of such a table of filters:

Fig. 2

NAME	SEQ	TYPE	OFFSET	VALUE (HEX)	COND	MATCH	FAIL	FWD	MON DEST	ADDL DEST
FLTR_001	1	LLC	0	AA.AA.03.00.00.00.81.37	EQ	2	255	NORM		
	2	LLC	16	04.52	EQ	3	255	NORM		
	3	LLC	22	00.07	EQ	0	255	ALT		2:3,2:4
FLTR_002	1	MAC	2	00.80.00.02.31.54	EQ	255	255	NORM	2:1	
FLTR_003	1	LLC	0	AA.AA.03.00.00.00.08.00	EQ	0	255	DROP		

ADD FILTER ADD SEQ DELETE SEQ

100. The figure above shows a table comprising three filters: FLTR_001 (having three stages), FLTR_002 (having one stage), and FLTR_003 (having one stage). FLTR_002 is a “MAC” type filter that operates on any message having the specified MAC address listed in the “VALUE (HEX)” column. Apple 1005 at 7:10-13. The other two filters are logical link control (LLC) filters that match data patterns in the LLC field. Apple 1005 at 7:32-43. The “FWD” column specifies the action that should be taken. NORM tells the filter to allow the message to proceed to its normal destination. DROP tells the filter to block the message by dropping it from the network so it does not reach its destination. ALT tells the filter to forward the message to an alternative destination. Apple 1005 at 9:7-20.

4. “(1) filters specifying immediate action, and”

101. Pitcher ’554 discloses filters that operate to block or allow access based on the network address of the message. For example, at Apple 1005 at 7:10-16, Pitcher ’554 discloses:

As another example, filter group 216 named FLTR_002 is comprised of one filter having a sequence number of 1. The filter forwards all packets destined to a device having a MAC address of 008000023154(hex) to a monitoring device or analyzer attached to module 2, port 1, in addition to the normal destination port. The last filter group 217, named FLTR_003, drops IP packets.

102. The MAC address is the address of the particular resource to which the message is addressed or from which the message originated on the network. In this example, the message is forwarded to the normal destination port (allowed) and is also forwarded to an additional monitoring device. Alternatively, as shown in the FLTR_003 example, the “FWD” column can be set to “DROP,” in which case, the message is blocked. Such a filter, which allows or blocks a message based on its network address, is a “filter specifying immediate action,” in the context of the ’033 patent.

5. “(2) filters specifying deferred action;”

103. Pitcher ’554 discloses filters that operate to block or allow messages based on matching content of the message to patterns or keywords defined in the filter. For example, Apple 1005 at 8:4-32 describes multiple comparisons that may be performed to match the content of a network message:

In one embodiment, each of the fields in the RIF are assigned a number. If the routing information indicator (RII) bit in the MAC

source address field is not set, the RIF type filter will fail. The number assigned to each field in the RIF may be as follows:

- 0--compare the value to the contents of the RT field;
- 1--compare the value to the contents of the length field;
- 2--compare the value to the contents of the largest frame size field;
- 3--compare the value to the contents of the first ring number in the RD fields (Note--the filter must take into consideration the value of the direction bit in order to determine in which order to read the RD field);
- 4--compare the value to the first bridge number;
- 5--compare the value to any ring number;
- 6--compare the value to any bridge number;
- 7--compare the value to the last bridge number; and,
- 8--compare the value to a bridge number, ring number pair, i.e., a route descriptor.

The value field 305 specifies in hexadecimal the value to compare with the contents of a data packet at the location within the packet determined by the value of the type and offset fields. The condition field 306 allows six types of comparisons. The value in the value field can be compared to the contents of a data packet at the offset specified to determine if the value is equal (EQ), not equal (NE), less than (LT), less than or equal to (LE), greater than (GT), or greater than or equal to (GE) the contents of the data packet.

104. This type of pattern matching, where patterns specified in the filter are compared to the content of the network message, other than address or port, is a “filter specifying deferred action” in the context of the ’033 patent.

6. **“(c) comparing information in the message to filtering information in at least one of said filters specifying immediate action and said filters specifying deferred action; and”**

105. Pitcher '554 discloses that information in the message is compared to filtering information. For example, at Apple 1005 at 8:4-32, which I quoted immediately above, Pitcher '554 describes that “[t]he value in the *value field can be compared to the contents of a data packet* at the offset specified to determine if the value is equal (EQ), not equal (NE), less than (LT), less than or equal to (LE), greater than (GT), or greater than or equal to (GE) the contents of the data packet.” (emphasis added). Thus, the filters disclosed in Pitcher '554 immediately block or allow a message destined for a particular address, for example, by comparing the MAC address of a message to a MAC address in the filter table, or can block or allow a message by comparing the value in the value field of the filter to other content in the message.

7. **(d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.**

106. Pitcher '554 discloses that the filter table, such as the one depicted at Figure 2, which is reproduced again below, includes a compare directive in the “COND” column, and an action in the “FWD” column to specify what should be done when the comparison condition is met. *See* Apple 1005 at 3:49-4:4; 9:5-20.

Fig. 2

NAME	SEQ	TYPE	OFFSET	VALUE (HEX)	COND	MATCH	FAIL	FWD	MON DEST	ADDL DEST
FLTR_001	1	LLC	0	AA.AA.03.00.00.00.81.37	EQ	2	255	NORM		
	2	LLC	16	04.52	EQ	3	255	NORM		
	3	LLC	22	00.07	EQ	0	255	ALT		2:3,2:4
FLTR_002	1	MAC	2	00.80.00.02.31.54	EQ	255	255	NORM	2:1	
FLTR_003	1	LLC	0	AA.AA.03.00.00.00.08.00	EQ	0	255	DROP		

ADD FILTER ADD SEQ DELETE SEQ

107. For example, looking at FLTR_002 in Figure 2, when the value specified in the “VALUE (HEX)” column is compared to the message and the “EQ” (equals) condition is true, the “FWD” (forward) column specifies that the message should proceed to the destination address, i.e., be allowed, based on the “NORM” (normal) action specified there. If, on the other hand, the FWD column contained the “DROP” action, that would indicate that the message should be blocked (dropped) if the comparison evaluated to true.

108. Based on the analysis above, it is my opinion that Pitcher ’554 anticipates claim 1.

N. Claim 2 Of The ’033 Patent Is Anticipated By Pitcher ’554

109. It is my opinion that Pitcher ’554 anticipates claim 2 of the ’033 patent, as I discuss in detail below.

1. “2. The method of claim 1, wherein some of the filters indicate that the message should be sent, and others indicate that the message should be blocked.”

110. Pitcher '554 discloses that the filter table includes a column specifying the action to be taken when a message matches the condition specified in the filter. At Apple 1005 at 9:5-19, Pitcher '554 states the following:

The fwd field 309 indicates the forwarding action to take with respect to a data packet whose contents match the value specified in value field 305 of the present filter. There are three values that may be specified to indicate the manner in which a packet is processed by the network device: NORM, DROP, and ALT. A value of normal (NORM) indicates the data packet is to be forwarded by the network device to the normal destination port, or ports as the case may be, as well as any destination ports specified in the monitor destination field (mon dest) 310 and the additional destination field (addl dest) 311. A value of drop (DROP) indicates the data packet is to be discarded by the network device. A value of alternate (ALT) indicates the data packet is to be forwarded, but only to the destination ports specified in the monitor destination and the additional destination fields. The packet is not to be forwarded to the normal destination port(s).

111. The value of “NORM” thus indicates that the message should be allowed. The value of “DROP” indicates that the message should be blocked. Thus, Pitcher '554 also anticipates claim 2.

O. Claims 15 And 23 Of The '033 Patent Are Anticipated By Pitcher '554

112. It is my opinion that Pitcher '554 anticipates claims 15 and 23 of the '033 patent. While claim 1 is directed at network messages that are sent from the client to the Internet resource, claim 23 is directed to messages arriving at the client from the Internet resource, and claim 15 does not specify the direction of the message. In other respects, these claims have essentially the same scope.

113. It is my opinion that Pitcher '554 anticipates claims 15 and 23 for the same reasons it anticipates claim 1 because it discloses that the filtering operations may be performed on messages travelling in either direction. For example, Pitcher '554 discloses at Apple 1005 at 3:53-65 that messages “*entering or exiting*” a port may be filtered and that data “*received or transmitted*” at a port may be filtered:

An embodiment of the present invention defines a pattern and performs a forwarding action specified for packets whose contents match or do not match the pattern, according to a specified condition. Such filters may be configured on a per port basis, i.e., a filter can be applied to data packets entering or exiting a specific port on a networking device such as a LAN switch. A data packet received or transmitted at a port of a network device whose contents meet a condition specified by a filter may be forwarded to a normal destination port according to normal forwarding rules, forwarded to additional destination ports, forwarded to a monitor destination port, dropped, or subjected to another filter.

114. Because the system of Pitcher '554 operates on messages that are both outgoing and incoming, it anticipates claims 15 and 23 for the same reasons it anticipates claim 1.

P. Claim 9 Of The '033 Patent Is Rendered Obvious By Pitcher '554 Or By Pitcher '554 In Light Of Baker '645.

115. It is my opinion that Pitcher '554 renders claim 9 obvious in light of the knowledge of one of ordinary skill in the art or, alternatively, in light of Baker '645.

1. **“9. The method of claim 1, wherein steps (a)-(d) are all performed by a client computer, step (b) including maintaining the database in storage residing on the client computer. ”**

116. The filtering operations in Pitcher '554 are performed on a local area network (LAN) switch. But Pitcher '554, at Apple 1005 at 5:8-12, indicates that the filtering could also be performed on other devices:

Referring to FIG. 1, a network device 100 as may be utilized by an embodiment of the present invention is shown. Network device 100 is a LAN switch, however, it is understood by those of ordinary skill in the art that an embodiment of the present invention may be applied to other network devices such as a hub or bridge.

117. It was well known in the art that LAN switches and bridges are used to isolate a local network from the larger Internet, and one of the benefits of doing so is conserving bandwidth on the LAN by eliminating unnecessary traffic. Pitcher '554 notes that at its logical end, partitioning a network into LANs finally results in a single

client workstation behind the LAN switch. At Apple 1005 at 1:27-34, Pitcher '554 states:

To continue satisfying the growing demands of client/server computing, networking devices such as bridges, routers, hubs, and LAN switches are installed. A common strategy to reduce traffic in a congested LAN is to segment the LAN into smaller LANs so that bandwidth is shared among fewer users. Carried to its end, segmentation results in each LAN having only one device attached, for example, a single server or workstation.

118. Once a LAN switch is controlling network traffic for a single client workstation, it would be more efficient to simply incorporate the functionality of the switch into the client itself. Thus, one of ordinary skill would have recognized that the filtering functions and databases disclosed in Pitcher '554 could have been implemented on the client workstation. The selection of where to locate this functionality was a natural matter of design choice between a thin client model and a thick client model. As I discussed earlier, the trade-offs between a thin client model and thick client model were well known in the art, with each architecture having advantages and disadvantages that would have to be balanced for the particular network architecture desired. Thus, one of ordinary skill would have known that implementing the filters of Pitcher '554 on a proxy server, on a LAN switch or router, or on a client computer, were all likely to be successful, and that the selected location was a matter of design choice. Therefore, it is my opinion that Pitcher '554 renders

claim 9 obvious because the choice of where to locate the filtering operations would have been a design choice between two known alternatives, would have involved the application of ordinary engineering skill, and would not have led to any unexpected results.

119. Alternatively, it would have been obvious to combine Pitcher '554 with Baker '645. Baker '645 discloses that filtering software can be implemented either on a client machine or a separate machine: “[a] program that controls access to remote resources will be termed a filter. A filter may be embodied in ***software running on the client machine*** or on a separate machine.” Apple 1002 at 1:29-32 (emphasis added); Apple 1004 at 1. The concept of thin and thick clients was not invented by Baker; rather, Baker '645 discloses that this was a trade-off that was well known in the art. One of ordinary skill would have been motivated to combine Pitcher '554 and Baker '645 because both are directed to solving the same problem: blocking or allowing network messages to or from Internet resources. Further, Baker '645 adds the enhanced functionality of filtering based on a ratings database, and one of ordinary skill would have been motivated to enhance Pitcher '554 by adding this functionality in order to achieve a more capable system.

120. Thus, in light of the teachings of Baker '645, it would have been obvious to locate the filtering operations and filter tables of Pitcher '554 on the client device. The combination of Pitcher '554 and Baker '645 renders claim 9 obvious.

Q. Overview Of Schloss '507

121. I understand that Schloss '507 (Apple 1006) was filed on July 5, 1995 and qualifies as prior art to the '033 patent. I have reviewed Schloss '507, and it is my opinion that it anticipates claims 1, 2, 9, 15, and 23 of the '033 patent.

122. Schloss '507 discloses a computer-implemented Internet filtering system that controls access to Internet resources. When a client requests a particular URL, the request is compared to a table of filters to determine whether or not the resource identified by the URL is appropriate for viewing. *See* Apple 1006 at 6:23-36. Two types of filters are disclosed by Schloss '507. The first type is the “AdviseOnURL” filter, which blocks or allows access to the “particular page of content data requested from the content server.” Apple 1006 at 6:20-23. This is an “immediate” filter in the context of the '033 patent because it controls access based on the network address of the resource.

123. The second type is the “AdviseOnURLIncludingLinks” filter. Such a filter scans the content of the data returned by the original request for a URL to see if the web page returned to the user contains links to other resources that may be inappropriate. At Apple 1006 at 6:23-28, Schloss '507 discloses, “[o]n the other hand, the command verb ‘AdviseOnURLIncludingLinks’ requests that the characterization data returned by the advisory server 20 that pertains to the particular page of content data requested from the content server 6 plus any content linked to the particular

page, for example, by a hypertext anchor within the page.” An

“AdviseOnURLIncludingLinks” filter is thus a “deferred” filter in the context of the ’033 patent because such a filter matches patterns in hypertext links included in the returned message in order to determine whether to allow or block the network message requesting a resource.

124. A detailed explanation of my opinion that Schloss ’507 anticipates claims 1, 2, 9, 15, and 23 of the ’033 patent follows.

R. Claim 1 Of The ’033 Patent Is Anticipated By Schloss ’507

1. Preamble: A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:

125. Schloss ’507 discloses a system for preventing or allowing access to Internet sites. In the Abstract of Apple 1006, it states, “In operation, each time data (e.g., a web page) is downloaded from a content server to the client, prior to display, the client sends a request signal to the advisory server asking that it advise the client on the content of the web page. The advisory server rates the page and sends a classification rating back to the client. The client thereafter displays or does not display the web page according to the classification rating based on the client's selected preferences.”

2. “(a) opening a data stream to send a message through an interface to an Internet server”

126. As I explained in my discussion of the Baker '645 reference, this limitation is inherently disclosed by any reference describing TCP/IP communications. Schloss '507 discloses this limitation at Apple 1006 at 4:30-36 because it discloses requesting web content over TCP/IP sockets: “More specifically, a client system running a Web Browser request [*sic*] content from a content server 6 using a Hypertext Transfer Protocol (HTTP) request and receiving the content in a HTTP response. HTTP requests and responses occur over TCP/IP sockets that are communicated over the communication link between the client 4 and the content server 6.”

3. “(b) maintaining a database of filtering information comprising a table of filters, said table comprising”

127. Schloss '507, at Apple 1006 at 4:57-5:7, discloses a database maintaining characterization information used to determine whether certain resources may be accessed:

According to the present invention, one or more advisory servers 20 (three shown) are interfaced to the Internet 8 as illustrated in FIG. 2. The advisory servers maintain one or more knowledge bases 22 that characterize the content generated by one or more of the content servers 6. In addition, the system includes one or more clients 25 (three shown) running a Web Browser that when set in an advisory mode, for each content request to the content servers 6, requests characterization data from one or more of the advisor

servers 20. The advisory servers 20 generate the appropriate characterization data based upon the information stored in the knowledge base 22, and transmit the characterization data to the client 25. Upon receiving the characterization data, the client 25 utilizes the characterization data to determine whether to filter the content data transmitted by the content server 6. In addition, the client may utilize the characterization data to generate additional information.

128. Thus, the client receives data from the advisory servers that it uses to decide whether or not to allow access to certain resources. The client is also able to “utilize the characterization data to generate additional information,” as quoted above, that can be used to filter the data transmitted by the content server. Thus, the client maintains information for filtering network messages.

4. “(1) filters specifying immediate action, and”

129. Schloss ’507, as I discussed above, discloses “AdviseOnURL” filters. “The command verb ‘AdviseOnURL’ requests that the characterization data returned by the advisory server 20 pertain to only the particular page of content data requested from the content server 6.” Apple 1006 at 6:19-23. Thus, access is granted or denied based only on the particular network address requested. This is therefore an example of an immediate filter in the context of the ’033 patent.

5. “(2) filters specifying deferred action;”

130. Schloss ’507 also discloses “AdviseOnURLIncludingLinks” filters. “On the other hand, the command verb ‘AdviseOnURLIncludingLinks’ requests that the characterization data returned by the advisory server 20 that pertains to the particular page of content data requested from the content server 6 plus any content linked to the particular page, for example, by a hypertext anchor within the page. In this case, the command verb indicates whether the request encoded within the advisory request signal is a ‘AdviseOnURL’ request or an ‘AdviseOnURLIncludingLinks’ request.” Apple 1006 at 6:23-32.

131. As discussed above, “AdviseOnURLIncludingLinks” filters search for and match data in the content returned by the server (such as embedded hypertext anchors) rather than filtering on port or network address of the network message. Thus, these filters are “deferred” filters in the context of the ’033 patent.

6. “(c) comparing information in the message to filtering information in at least one of said filters specifying immediate action and said filters specifying deferred action; and”

132. Schloss ’507 discloses that the URL in the message requesting content is compared with characterization information retrieved from an advisory server to determine whether to block or allow the request. “[I]f the character data returned from the advisory server indicates the data is offensive to minors, the client 25 may inhibit loading of the content data.” Apple 1006 at 5:66-6:1. In other words, if the

requested URL matches a URL for which there is negative characterization data, the message requesting that resource will be blocked.

7. (d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.

133. In the Abstract, Schloss '507 discloses that “[t]he advisory server rates the page and sends a classification rating back to the client. The client thereafter displays or does not display the webpage according to the classification rating based on the client’s selected preferences.” Further, at Apple 1006 at 5:60-63, Schloss '507 discloses that “the client may inhibit loading of or load the content data associated the contour request as a function of the received characterization data.” In other words, based on the comparison of the requested URL to URLs in the filter list having associated characterization data, the system can prevent or allow the transmission requesting that resource, based on the selected preferences of the client.

134. Based on the analysis above, it is my opinion that Schloss '507 anticipates claim 1 of the '033 patent.

S. Claim 2 Of The '033 Patent Is Anticipated By Schloss '507

135. It is my opinion that Schloss '507 anticipates claim 2 of the '033 patent, as I discuss in detail below.

1. **“2. The method of claim 1, wherein some of the filters indicate that the message should be sent, and others indicate that the message should be blocked.”**

136. According to Schloss, the “client’s selected preferences” specify whether messages should be allowed or blocked. At the Abstract, it discloses “[t]he advisory server rates the page and sends a classification rating back to the client. The client thereafter displays or does not display the webpage according to the classification rating based on the client’s selected preferences.” Apple 1006 at Abstract.

Preferences can therefore be set for each filter to determine whether it will block or send messages.

T. Claim 9 Of The '033 Patent Is Anticipated By Schloss '507

1. **“9. The method of claim 1, wherein steps (a)-(d) are all performed by a client computer, step (b) including maintaining the database in storage residing on the client computer. ”**

137. Schloss '507 states at Apple 1006 at 11:56-58, “[a]s described above, the invention is embodied in a client running a Web Browser adapted to communicate with one or more advisory servers.” To the extent certain filtering information is maintained in an advisory server, Schloss '507 discloses that it is also possible for the client to create a new filtering database locally, based on the retrieved information: “[u]pon receiving the characterization data, the client 25 utilizes the characterization data to determine whether to filter the content data transmitted by the content server

6. In addition, the client may utilize the characterization data to generate additional information.” *Id.* at 5:2-7.

U. Claims 15 And 23 Of The '033 Patent Are Anticipated By Schloss '507

138. Claims 15 and 23 of the '033 patent are essentially commensurate in scope with claim 1 except that claim 1 is directed to outgoing (client to server) messages while claim 23 is directed to incoming (server to client) messages, and claim 15 does not specify a direction.

139. Schloss '507 discloses that outgoing requests are filtered, for example, when “AdviseOnURL” filters are used. *See, e.g.*, Apple 1006 at 6:12-36. Filters are also applied to data returned from an Internet server using

“AdviseOnURLIncludingLinks” filters to examine the content returned by an Internet server. The data examined includes “content linked to the particular page, for example, by a hypertext anchor within the page.” *Id.* at 6:27-29. Schloss '507 therefore discloses applying filters to both outgoing and incoming messages. Thus, Schloss '507 anticipates claims 15 and 23 for the same reasons it anticipates claim 1.

VII. CONCLUSION

140. Based on the foregoing, it is my opinion that claims 1, 2, 9, 15, and 23 of the '033 Patent are invalid over the prior art discussed above.

141. 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 the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

142. I reserve the right to supplement my opinions in the future to respond to any arguments that the patent owner raises and to take into account new information as it becomes available to me.

143. I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true and that such statements are made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: March 27, 2015

A handwritten signature in black ink, appearing to read "Charles D. Knutson", with a long horizontal flourish extending to the right.

Charles D. Knutson, Ph.D.