UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

OpenTV, Inc.,
Patent Owner.

Case No. _____

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 5,884,033 CHALLENGING CLAIMS 1, 2, 9, 15, and 23 UNDER 35 U.S.C. § 312, 37 C.F.R. § 42.104

TABLE OF CONTENTS

LIST OF EXHIBITS

Apple 1001 -- U.S. Patent No. 5,884,033 ("the '033 Patent")

Apple 1002 -- U.S. Patent No. 5,961,645 ("Baker '645")

Apple 1003 -- U.S. Patent No. 5,696,898 ("Baker '898")

Apple 1004 -- U.S. Provisional App. No. 60/004,670 ("Baker '645 Provisional")

Apple 1005 -- U.S. Patent No. 5,790,554 ("Pitcher '554")

Apple 1006 -- U.S. Patent No. 5,706,507 ("Schloss '507")

Apple 1007 -- Prosecution File History for Application No. 08/645,636, which later issued as U.S. Patent No. 5,883,033 ("'033 File History")

Apple 1008 -- OpenTV's Infringement Contentions directed to Mac OS X Products ("Mac OS Contentions")

Apple 1009 -- OpenTV's Infringement Contentions directed to AppleTV Products ("AppleTV Contentions")

Apple 1010 -- Declaration of Dr. Charles D. Knutson ("Knutson Decl.")

Apple 1011 -- Curriculum Vitae of Dr. Charles D. Knutson

I. INTRODUCTION

Pursuant to 37 C.F.R. § 42.100, *et seq.*, Apple Inc. ("Petitioner") hereby petitions the United States Patent and Trademark Office (the "Office") to institute an *inter partes* review of Claims 1, 2, 9, 15, and 23 of U.S. Patent No. 5,884,033 ("the '033 Patent"). The '033 Patent, a copy of which is provided as Apple 1001, is assigned to OpenTV, Inc. ("Patent Owner"). The '033 Patent claims a method of filtering Internet traffic to selectively allow or deny access to certain Internet resources. As set forth below, the claimed invention is anticipated or rendered obvious by several prior art references. This petition presents several non-cumulative grounds of invalidity based on prior art that was not considered by the Office during prosecution. These grounds of invalidity are each reasonably likely to prevail, and this petition, accordingly, should be granted on all grounds.

II. GROUNDS FOR STANDING AND FEE AUTHORIZATION

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '033 Patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review on the grounds identified herein. This petition is timely filed under 37 C.F.R. § 42.102(a)(2) (the '033 Patent is not a patent described in section 3(n)(1) of the Leahy-Smith America Invents Act).

Pursuant to 37 C.F.R. § 42.103(a), the Office is authorized to charge an amount in the sum of $23,000 to Deposit Account No. 50-0639 for the fee set forth in 37

C.F.R. § 42.15(a), and any additional fees that might be due in connection with the Petition.

III. MANDATORY NOTICES (37 C.F.R. § 42.8)

Real Party-In-Interest: The real party-in-interest is Apple Inc.

Notice of Related Matters: OpenTV, Inc. has asserted this patent against Apple Inc. in Case No. 3:14-cv-01622-HSG, which was filed on April 9, 2014, and is currently pending in the District Court for the Northern District of California.

Petitioner's Lead and Back-up Counsel:

Lead Counsel: Mark E. Miller (Reg. No. 31,401), O'Melveny & Myers LLP, Two Embarcadero Center, 28th Floor, San Francisco, CA 94111. (Telephone: 415-984-8700; Fax: 415-984-8701; Email: markmiller@omm.com.)

Backup Counsel: Brian M. Cook (Reg. No. 59,356), Xin-Yi Zhou (Reg. No. 63,366), John Kevin Murray (Reg. No. 69,529), Anne E. Huffsmith (Reg. No. 57,041), and Ryan K. Yagura (Reg. No. 47,191), O'Melveny & Myers LLP, 400 S. Hope Street, Los Angeles, CA 90071. (Telephone: 213-430-6000; Fax: 213-430-6407; Emails: bcook@omm.com, vzhou@omm.com, kmurray2@omm.com, ahuffsmith@omm.com, and ryagura@omm.com).

Service Information: Service of all documents may be made to the lead counsel and backup counsel at O'Melveny & Myers LLP, Two Embarcadero Ctr. 28th Floor, San Francisco, CA 94111-3823, with courtesy copies to the following email addresses: markmiller@omm.com, bcook@omm.com, vzhou@omm.com,

kmurray2@omm.com, ahuffsmith@omm.com, and ryagura@omm.com. Petitioner's counsel may also be reached by telephone at 415-984-8700 and by facsimile at 415-984-8701.

IV. SUMMARY OF CHALLENGES

Petitioner challenges the patentability of Claims 1, 2, 9, 15, and 23 on the following grounds, which are described in detail in Section VI, below.

A. U.S. Patent No. 5,961,645 ("Baker '645") anticipates Claims 1, 2, 9, 15, and 23.

B. U.S. Patent No. 5,696,898 ("Baker '898") anticipates Claims 1, 2, and 15 and renders obvious Claims 9 and 23 either alone, or in combination with Baker '645.

C. U.S. Patent No. 5,790,554 ("Pitcher '554") anticipates Claims 1, 2, 15, and 23.

D. Pitcher '554 alone, or in combination with Baker '645, renders obvious Claim 9.

E. U.S. Patent No. 5,706,507 ("Schloss '507") anticipates or renders obvious Claims 1, 2, 9, 15, and 23.

V. THE CHALLENGED PATENT

A. Overview Of The '033 Patent

The '033 Patent was filed on May 15, 1996 and makes no claim of priority to any other application. Apple 1001 at cover. The claims are directed to a method of

filtering communications sent over the Internet to selectively block or allow access to certain Internet sites. *Id.* at 1:27-29; Claims 1, 15, 23. The alleged invention operates within a network environment in which communications between computers are governed by a protocol known as Transmission Control Protocol/Internet Protocol (TCP/IP). *Id.* at 2:42-50. TCP/IP was in use well before 1996, and the '033 Patent notes that the "current version" of Internet Protocol in 1996 was version 4. *Id.* at 2:51. The well-known and widely used Internet Protocol assigns each computer connected to the Internet an "IP address" of the form "n1.n2.n3.n4," where each "nx" is an 8-bit number (i.e., a number whose value can range from 0 to 255). *Id.* at 2:51-55. "To initiate communications with another computer over the Internet, a computer opens a port in its interface for a TCP data stream." *Id.* at 2:58-60; Apple 1010 at ¶¶ 48-49.

Users can access resources at a particular IP address using a more user-friendly "uniform resource locator" or "URL," which is text string of the form "http://www.name.ext." Apple 1001 at 2:67-3:4. A network server called a "domain name system" server or "DNS" server,[1] uses the domain portion of the URL string identifying a resource to look up its associated numeric IP address. *Id.* at 3:13-19. A user can request access to an Internet resource by, for example, typing

[1] The '033 patent refers to "DNS" as a "domain name server," although DNS is generally known in the art to stand for "domain name system."

"http://www.name.ext" into a web browser, where "http" refers to Hypertext Transfer Protocol, a protocol within the TCP/IP protocol suite. *Id.* at 2:42-48, 2:66-3:4. In response to such a request, the TCP/IP protocol engine looks up the IP address in the DNS server and "[t]he client opens a TCP data stream and uses this IP address to communicate with the other computer." *Id.* at 3:18-19.

Some materials accessible on the Internet may be objectionable, and it may be desirable to block or otherwise control access to certain Internet resources. Accordingly, the alleged invention of the '033 Patent provides a method for filtering messages sent over a network such as the Internet. *Id.* at 1:8-16. The claimed invention operates on messages exchanged via TCP/IP by comparing their content with information retrieved from a "database of filtering information" which specifies conditions under which certain transmissions should be allowed or denied. *Id.* at Claims 1, 15, 23.

The '033 Patent describes two types of filtering actions: direct actions and deferred actions. Apple 1001 at 4:14-20. "Direct actions indicate that the system should unconditionally allow or unconditionally block the transmission." *Id.* To perform the described direct actions, the claimed filtering system checks a database to retrieve filters based on the port number and/or IP address associated with the message:

> 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.

Id. at 4:43-50.

Deferred actions, on the other hand, require examining information other than the port number and IP address, for example:

> Deferred filter entries [in the database] 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 transmission.

Id. at 5:8-15. The '033 Patent provides an example of how direct (immediate) and deferred filters might be used when a user requests "http://www.domain/test.html" using a browser. *Id.* at 6:10-28. In this example, the DNS server returns the IP address 1.2.3.4 corresponding to the domain. *Id.* at 6:12-14. The system then looks for immediate filters: "[i]f 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" *Id.* at 6:16-18. If there is no immediate filter, a deferred filter may search for the pattern "test.html" in the outgoing data stream and decide whether to block the transmission based on the results of that pattern match. *Id.* at 6:19-28. As

another example of pattern matching, the '033 Patent notes that certain deferred filters might be configured to allow transmission of a character string containing "sextet" while blocking a character string containing "sex" by itself. *Id.* at 6:32-34. Wildcard characters, like "*" may also be used, such that the filter pattern "*XXX*" would match any instance of "XXX" in the message, whether proceeded or followed by any other character. *Id.* at 6:37-42.

As described in the '033 Patent, filtering operations can be applied to outgoing messages from the client to the Internet server, to incoming messages from the Internet server to the client, or both. Independent Claim 15 of the '033 Patent refers generally to "messages transmitted over the Internet," regardless of their direction. Independent Claim 1 is directed to "outgoing" transmissions from the client to the server. Independent Claim 23 is directed to "incoming" transmissions. Otherwise, the scope of these three independent claims is essentially identical. The table below compares the language of Claims 1, 15, and 23 to illustrate their similarity. Key differences are highlighted. Note that Claim 15 does not include the limitation of "opening a data stream . . ." However, as discussed above, opening a data stream is inherent to TCP/IP communications.

Claim 1	**Claim 15**	**Claim 23**
1. A method for communicating with servers over the Internet to	15. A method for filtering messages transmitted over the Internet to prevent or	23. A method for communicating with servers over the Internet to

prevent or allow access to Internet sites, the method comprising computer-implemented steps of:	allow access to Internet sites, the method comprising computer-implemented steps of:	prevent or allow access to Internet sites, the method comprising the computer-implemented steps of:
(a) opening a data stream to ***send a message*** through an interface to an Internet server;	--	(a) opening a data stream to ***receive a message*** through an interface from an Internet server;
(b) maintaining a database of filtering information comprising a table of filters, said table comprising	(a) maintaining a database of filtering information comprising a table of filters, said table comprising	(b) maintaining a database of filtering information comprising a table of filters, said table comprising
(1) filters specifying immediate action, and	(1) filters specifying immediate action, and	(c) filters specifying immediate action, and
(2) filters specifying deferred action;	(2) filters specifying deferred action;	(d) filters specifying deferred action;
(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	(b) 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	(e) comparing information in the message to filtering information in the filters specifying immediate action and filters specifying deferred action and
(d) determining whether to prevent or allow the ***outgoing transmission*** of	(c) determining whether to prevent or allow ***transmission*** of the	(f) determining whether to prevent or allow the ***incoming transmission***

the message based on the comparison.	message in response to the comparison.	of the message based on the comparison.

Typically, an "outgoing transmission" would be an HTTP request including a URL, as described above. Thus, the transmission could either be unconditionally blocked or allowed by comparing the URL domain name to a list of domain names in an "immediate filter," or additional comparisons could be made, for example, by comparing character strings within the URL to patterns specified in "deferred" filters to decide whether to block or allow the transmission. For an incoming transmission, content of the incoming message (which might also include a redirected URL) would be compared with immediate and deferred filters.

Dependent Claim 2 recites:

> 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.

And dependent claim 9 specifies that the steps of claim 1 are performed on the client computer, which would generally be the user terminal running the browser or other software that makes a request for an Internet resource:

> 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.

Systems for performing the claimed filtering steps were well known in the art by May 15, 1996, as described in detail below. Multiple references described below,

which were not before the Office during prosecution, anticipate or render obvious '033 Patent Claims 1, 2, 9, 15, and 23.

B. Level Of Ordinary Skill In The Art

The level of ordinary skill in the art is evidenced by the references cited in Section VI below. More specifically, one of ordinary skill in the art 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. Apple 1010 ¶ 41. A hypothetical person having ordinary skill in the art shall be referred to herein as a "PHOSITA."

C. Summary Of The Prosecution History Of The '033 Patent

None of the references relied upon in this petition was before the Office during prosecution of Application No. 08/645,636 ("the '636 Application"), which later issued as the '033 Patent. The '636 Application was filed on May 15, 1996 with 26 claims, four of which were independent. Apple 1007.002.

On June 27, 1997, the Examiner rejected all claims as anticipated or obvious over U.S. Patent No. 5,606,668 to Shewd. Apple 1007.046. The Examiner explained that Shewd discloses an Internet packet filtering system, including "generating/maintaining a database of filtering information for the packet filters (figures 3a, 3b) including service names, ports, network addresses and actions to be taken." Apple 1007.048. The Examiner acknowledged, with respect to certain

dependent claims, that Shewd does not disclose maintaining the filter information on the client machine. Apple 1007.050. The Examiner found, however, that implementing filters on the client would have been obvious because it "would have provided storage for storing filtering instructions for various levels of protection and/or different filtering capability at the client workstation." *Id.*

In response to the rejection, the Applicants initiated an in-person interview with the Examiner on January 7, 1998 to discuss the Shewd reference. Apple 1007.055. Then, on January 22, 1998, the Applicants amended Claim 1 to further limit the "database of filtering information" by requiring both "immediate action" and "deferred action" filters as follows:

> 1. (Amended) A method for communicating with servers over the Internet, the method comprising computer-implemented steps of:
> (a) opening a datastream to send a message through an interface to an Internet server;
> (b) maintaining a database of filtering information <u>comprising a table of filters, said table comprising</u>
> <u>(1) filters specifying immediate action, and</u>
> <u>(2) filters specifying deferred action;</u>
> (c) comparing information in the message to filtering information in the database; and
> (d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.

Apple 1007.058-59. Similar limitations were added to independent Claim 15 and included in new independent Claim 33 (issued as Claim 23). The Applicant explained the significance of these added limitations as follows:

> These fundamental differences between the Schwed [*sic*] network security system and Applicants' filtering methods are further illustrated in the operation of the two types of filters in Applicants' methods. Schwed [*sic*] does not disclose the use of immediate action and deferred action filters as embodied in Applicants' methods. The deferred action filters in Applicants' methods include additional fields, such as a keyword field, a filter pattern field, a directional indicator field, or a compare directive field, that are neither disclosed nor suggested by Schwed [*sic.*]. See specification, p. 8 11.17-28. The ***presence of these filters together with the direct action filters allows the type of highly selective filtering*** that is characteristic of Applicants' invention.

Apple 1007.064-65 (emphasis added). In other words, the internet packet filtering system of Shewd, according to the Applicants, lacked the ability to perform pattern matching on fields, other than port and address, and thus did not disclose the "deferred action" filters added by amendment.

The Applicants also argued that the claimed filters operate "between the presentation and application levels (layers 6 and 7, respectively) of the seven-level ISO protocol model," as opposed to Shewd, which discloses filtering at lower levels of the protocol stack. Apple 1007.064. However, the Applicants did not cite any support in the specification for this distinction and did not amend the claims to include this

limitation. *Id.* In fact, this argument is directly contradicted by dependent claims 3 and 4, which depend from claim 1 (as discussed in more detail below in the section on claim construction). *See also* Apple 1010 ¶ 36.

On March 25, 1998, evidently rejecting the argument that Shewd was irrelevant because of the protocol stack layer at which it operates, the Examiner again rejected all claims as obvious over the combination of Shewd with U.S. Patent No. 5,618,648 to Canale, which teaches sorting email by filtering its content and metadata. Canale teaches filters used to automatically sort electronic mail, which the Examiner found to disclose the "deferred action" filters of the pending claims. Apple 1007.072. In other words, the keyword/pattern matching disclosure of Canale satisfied the "deferred action" filter limitations, and, when combined with Shewd's IP packet filters ("immediate action" filters), rendered the independent claims obvious.

The Applicants again initiated an in-person interview with the Examiner on July 2, 1998 to discuss the prior art, Apple 1007.077, and then further amended Claim 1 as follows:

> 1. (Twice Amended) A method for communicating with servers over the Internet <u>to prevent or allow access to Internet sites</u>, the method comprising computer-implemented steps of:
> (a) opening a datastream to send a message through an interface to an Internet server;
> (b) maintaining a database of filtering information comprising a table of filters, said table comprising

(1) filters specifying immediate action, and

(2) filters specifying deferred action;

(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 ~~the database~~; and

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

Apple 1007.081. Corresponding amendments were made to independent Claims 15 and 33 (issued as Claim 23). The Applicants distinguished Canale, which filters emails by content, sender, etc., from the claimed filters that "prevent or allow access to Internet sites." The Applicants further stated "neither Schwed [*sic.*] nor Canale et al. provides a suggestion to combine immediate action filters with deferred action filters, nor is there any teaching that making that combination in the manner claimed can be used to both allow access to desired Internet sites and prevent access to undesired Internet sites." Apple 1007.084.

Following a third rejection directed to claims not at issue in this Petition, the Examiner allowed the '636 Application on September 18, 1998. Apple 1007.110.

D. Claim Construction

In the context of an *inter partes* review, a claim in an unexpired patent is to be given its broadest reasonable construction in light of the specification in which it appears. 37 C.F.R. § 42.100(b); *see also In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984). The '033 Patent has not expired. Thus, for the purpose of this proceeding, the

claims of the '033 Patent should be given their broadest reasonable interpretation. For terms not specifically listed and construed below, Petitioner interprets them for purposes of this review in accordance with their plain and ordinary meaning under the broadest reasonable interpretation. Because this standard is different than the claim construction standard used in litigation, *see In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364, 1369 (Fed. Cir. 2004), Petitioner expressly reserves the right to argue in litigation a different construction for any term recited by the claims of the '033 Patent.

Pursuant to § 42.100(b), and solely for purposes of this review, Petitioner proposes the following broadest reasonable constructions:

1. "filters specifying immediate action" (Claims 1, 15, 23)

The broadest reasonable construction of "filters specifying immediate action" is "filters specifying whether transmission of the message should be allowed or blocked based on a port number or network address specified in the message." Apple 1010 ¶¶ 32-37.

The '033 Patent specification does not expressly use the term "filters specifying immediate action." But it states that actions specified by the filters are "divided into two groups, direct action or deferred action. Direct actions indicate that the system should unconditionally allow or unconditionally block the transmission." Apple 1001 at 4:14-17. It then states that filter entries "are first scanned for entries that require direct action: if there are any, these actions are carried out immediately." *Id.* at 4:18-20. The use of "immediate action" filters is described as follows:

> 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).

Apple 1001 at 4:39-55. Apple 1010 ¶¶ 32-37. Further, a filter may be set to block or allow any port or any IP address by entering "ANY PORT" or "ANY IP" in the filter. Thus, a filter requiring immediate action may specify a port number and/or network address and indicate whether the message should be allowed or blocked. The example quoted above specifically identifies the network address as an "IP address," but the '033 specification elsewhere describes that Internet resources may also be accessed by specifying a URL or "domain name," which are alternative ways of specifying the location of a resource available over the Internet. *See* Apple 1001 at 2:63-3:19. Indeed, Claim 3 depends from Claim 1 and further limits immediate action filters as follows: "the filters specifying immediate action comprise fields specifying an

interface port, and Internet Protocol (IP) address, and an action to be taken if the filtering information matches the information in the message." Because Claim 3 is presumed to further limit parent Claim 1, the address specified by an immediate action filter must be broader than just an IP address. Claim 6 depends from Claim 1 (via Claim 5), and recites comparing a "domain name in the URL" to immediate action and deferred action filters. Based on differences between claims 1 and 6, immediate action filters must encompass at least IP addresses, URLs, and domain names as ways of specifying a location of a resource on the Internet. Thus, "filters specifying immediate action" should be construed as "filters specifying whether transmission of the message should be allowed or blocked based on a port number or network address specified in the message." Apple 1010 ¶¶ 32-37.

The patentee during prosecution argued that the claimed filters operate "between the presentation and application levels (layers 6 and 7, respectively) of the seven-level ISO protocol model." Apple 1007.064. In addition to having no support in the specification, this argument is directly contradicted by claims 3 and 4, which depend from claim 1. Claim 3 further limits "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 includes "comparing an Internet Protocol (IP) address." Internet Protocol (IP) addresses are well known to be part of layer 3 (network layer) of the seven-level ISO protocol model and not part of layer 6

or 7, so "filters specifying immediate action" cannot be limited as the patentee argued during prosecution. Apple 1010 at ¶ 36; *See Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP*, 616 F.3d 1249, 1255 (Fed. Cir. 2010) ("A patent claim construction that renders asserted claims facially nonsensical cannot be correct.").

2. "filters specifying deferred action" (Claims 1, 15, 23)

The broadest reasonable construction of "filters specifying deferred action" is "filters specifying whether transmission of the message should be allowed or blocked based on information in the message other than a port number or network address." Apple 1010 ¶¶ 32-37.

The '033 Patent requires that deferred action filters perform additional pattern matching. For example:

> 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 transmission.

Apple 1001 at 5:8-15. As described in the specification:

> [W]hen data is transmitted over an open TCP/IP connection, the direction of the transmission is compared to the directional indicators in the deferred entities (step 130). For each entry in a filter that matches the direction, the beginning of the data stream is

> compared to the keyword in the filter entry (step 132). If the keywords match (step 134), the data is further compared to the filter pattern of the filter(s) according to the compare directive (step 136).

Id. at 5:20-28. The requirement of additional pattern matching is reinforced by an example of immediate action and deferred action filters operating together:

> As an example of blocking an HTTP transmission, assume that the user requests "http://www.domain/test.html." The client transmits the URL request and the domain name server returns an IP address, e.g., 1.2.3.4, corresponding to the domain name. The client tries to open a TCP/IP connection with that IP address and typically with port 80. If that IP address and port 80 (or that IP address with ANY PORT) are together in a BLOCK filter, the system prevents the data stream from opening.
>
> Rather than specifying blocking at this time, a filter can indicate a deferred action. In this example, the filter searches for a GET command as the keyword in an outgoing data stream, and for "test.html" as the filter pattern in the transmission. When the client sends a transmission with a GET command to get information under the directory test.html, the host server will respond with data for that directory. But if there is a blocking filter for test.html, the system can block the incoming data by discarding it or replacing it.

Id. at 6:10-28. The difference between immediate action filters and deferred action filters is that deferred action defines additional pattern-matching or keyword-matching steps beyond just examining the network address. Apple 1010 ¶¶ 32-37.

Although the terms "immediate" and "deferred" might suggest a temporal relationship between these types of filters, the language of claim 1 neither requires nor allows for any temporal relationship between the two filter types. Claim 1 recites "comparing information in the message to filtering information in at least one of said filters specifying immediate action and said filters specifying deferred action." The claim, therefore, would cover comparing the message to a deferred filter without ever comparing it to an immediate filter, demonstrating there is no required time order. Further, all comparisons must be made before a message can be allowed or blocked, so no comparison can be "deferred" until later. Independent claims 15 and 23 include similar language. What differentiates immediate from deferred filters is that the former looks at network address or port number, while the latter matches data in other parts of the message. The broadest reasonable construction of "filters specifying deferred action" is "filters specifying whether transmission of the message should be allowed or blocked based on information in the message other than a port number or network address." Apple 1010 ¶ 37.

3. "Internet sites" (Claims 1, 15, 23)

The broadest reasonable construction of "Internet sites" is "resources accessible on the Internet using TCP/IP." Apple 1010 ¶ 38.

The '033 Patent is entitled "Internet Filtering System for Filtering Data Transferred over the Internet Utilizing Immediate and Deferred Filtering Actions."

Consistent with its title, the patent describes applying filters to block or allow messages transmitted over the Internet:

> 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.

Apple 1001 at 2:41-50; Apple 1010 ¶¶ 39-40. The Internet sites contemplated by the '033 Patent are resources that can be accessed using TCP/IP protocols, such as those listed above. Therefore, "Internet sites" should be construed as "resources accessible on the Internet using TCP/IP."

VI. SPECIFIC GROUNDS FOR INVALIDITY

A. Claims 1, 2, 9, 15, And 23 Are Anticipated By U.S. Patent No. 5,961,645 ("Baker '645").

Baker '645 (attached as Apple 1002) was filed on October 1, 1996 and claims priority to U.S. Provisional Application No. 60/004,670 ("Baker645 Provisional") (attached as Apple 1004), filed October 2, 1995. Baker '645 was not of record during prosecution of the '033 Patent. Baker '645 qualifies as prior art to the '033 Patent at least under 35 U.S.C. § 102(e) and addresses the same problem the '033 Patent purports to address:

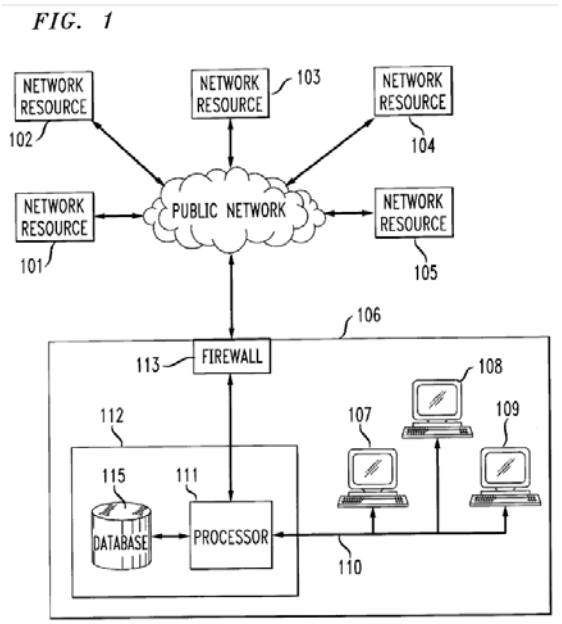
> A number of systems and methods have been proposed or created to control access to remote resources publicly available to users of other computers through the collection of networks known as the Internet. . . . A program that controls access to remote resources will be termed a filter. A filter may be embodied in software running on the client machine or on a separate machine.

Apple 1002 at 1:18-33; Apple 1010 ¶ 44.

As shown in Figure 1, below, the Baker '645 system maintains 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. *Id.* at 4:1-16. The filter database can be implemented either on the proxy server or on the client terminals:

> 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."

Id. at 3:62-67; Apple 1010 ¶ 52.



The database specifies which public network, e.g., Internet, resources, URLs, the client has permission to access:

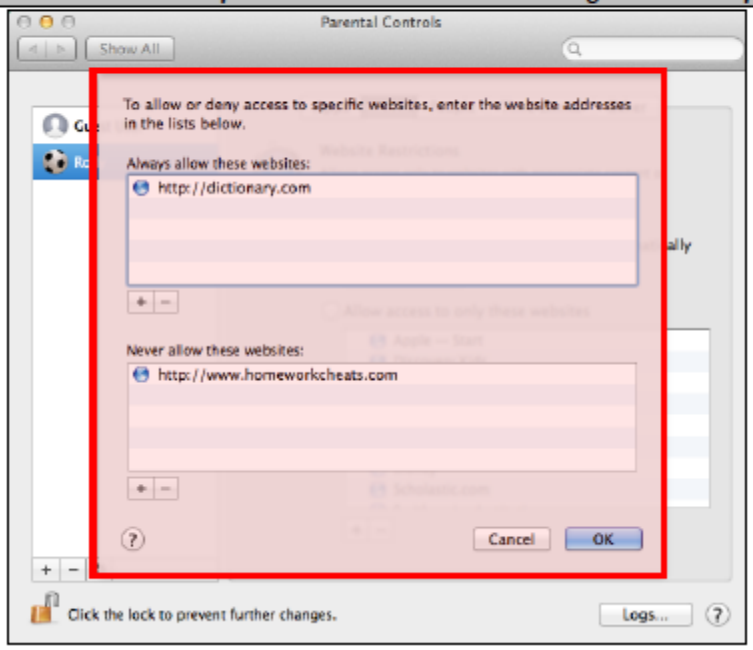
> The database 115 stores information about the network resources 101-105, in the form of URLs, and the user terminals 107-109 in the form of terminal IDs. The processor 111 can query the database 115 before allowing a terminal to receive a particular URL. For example, the database 115 may store a list 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.

Id. at 4:11-21. When a client sends an HTTP request for a specific URL, that URL is compared to the list of URLs in the filter database to determine whether the request will be sent; in other words, this is an "immediate action" filter. The Patent Owner's infringement contentions in the related litigation demonstrate that OpenTV believes such a listing of URLs constitutes a "filter specifying immediate action," as shown

below, where it accuses a list of "always allowed" websites and "never allowed" websites as meeting the limitations of filters specifying immediate action.

Exhibit D: Preliminary Infringement Contentions for U.S. Patent No. 5,884,033

	Representative Evidence of Infringement for Apple's Mac OS Products



Apple 1008.0017.

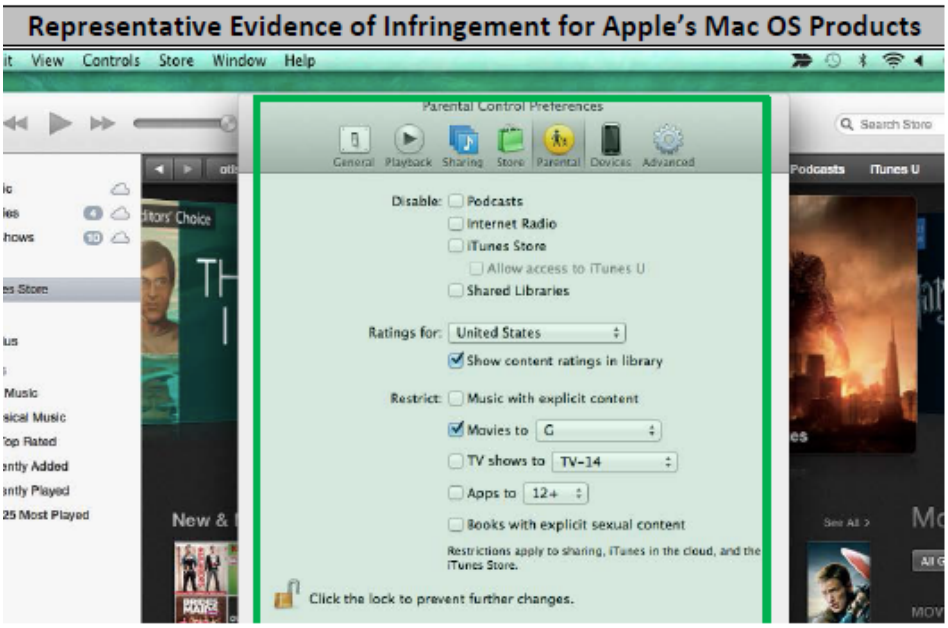
In addition to allowing or denying access based on just the URL, the filtering algorithm described in Baker '645 can alternatively examine additional data, such as a content rating, and allow or deny access based on matching that additional data, thus implementing a "deferred action" filter:

> 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.

Id. at 4:21-27; Apple 1010 ¶ 53. For example, a certain terminal may be allowed to retrieve only PG and G rated movies. If a resource responds with a message including metadata indicating an "R" rating, the "R" would be compared to the rating filter and the message would be blocked by the deferred action filter. Again, the Patent Owner's infringement contentions in the related litigation explicitly accuse just such content rating systems as examples of "deferred action" filters. *See, e.g.,* Apple 1009.0014 (excerpt) (comparing Apple TV's "Restrict Movies to G" feature to the '033 Patent's "deferred action" filter limitation):

See, also Apple 1008.0020 (excerpt) (comparing Apple iTunes "Restrict Movies to G" feature to the '033 Patent's "deferred action" filter limitation):



Baker '645 discloses as an alternative to content ratings that filters may be configured to match keywords in the message; this is another method of performing "deferred" filtering:

> The 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.

Apple 1002 at 5:26-30 (emphasis added). Thus, the Baker '645 system can also filter by matching patterns to a database of keywords, which would also be a "deferred" filter in the context of the '033 patent. Apple 1010 ¶ 54.

Filtering is performed not only on outgoing requests but also on incoming messages from the server back to the client: Baker '645 explains that when a URL

request is sent, the resource may respond by sending back a new URL for a variety of reasons, such as when a resource has been moved, or when the first resource includes CGI code for computing a new URL to return to the requestor. Apple 1002 at 2:16-37. The filter operations may be performed on either the outgoing URL or the incoming new URL:

> 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***.

Id. at 3:24-34 (emphasis added). Thus, Baker '645 teaches filtering on both outgoing and incoming messages.

The chart below shows in detail how Baker '645 discloses each and every limitation of each challenged claim. Each citation is followed by citations to the Baker '645 Provisional application (Apple 1004), demonstrating support in the earlier-filed application. With respect to element 1(a), "opening a data stream . . ." (and the corresponding element 23(a)), it should be noted that that the '033 Patent admits that opening a data stream is an inherent part of using TCP/IP to access an Internet server. *See* Apple 1001 at 3:18-19; Apple 1010 ¶¶ 48-49. That function is therefore

inherently disclosed by any reference that contemplates sending and receiving

TCP/IP messages.

1. A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:
Apple 1002 at 1:12-25 ("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')."); *see also* Apple 1004.0007; Apple 1010 ¶¶ 46-47.
(a) opening a data stream to send a message through an interface to an Internet server;
Apple 1002 at 1:48-54 ("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."); *see also* Apple 1004.0009; Apple 1010 ¶¶ 48-49. Inherent. *See* Apple 1001 at 3:18-19; Apple 1010 ¶¶ 48-49.
(b) maintaining a database of filtering information comprising a table of filters, said table comprising
Apple 1002 at 4:11-21 ("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."); *see also* Apple 1004.0010; Apple 1010 ¶¶ 50-51.
(1) filters specifying immediate action, and
Apple 1002 at 4:14-21 ("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."); *see also* Apple 1004.0010; Apple 1010 ¶ 52.
(2) filters specifying deferred action;
Apple 1002 at 4:21-27 ("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."); *see also* Apple 1004.0010; Apple 1010 ¶ 53. Apple 1002 at 5:26-30 ("The 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."); *see also* Apple 1004.0010; Apple 1010 ¶ 54. Apple 1004.0009 ("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."); *see also* Apple 1002 at 3:24-35; Apple 1010 ¶ 54.
(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
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 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."); *see also* Apple 1004.0009-10; Apple 1010 ¶ 56. Apple 1002 at Claim 6 ("6. A public network resource access system comprising . . . 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;") Apple 1002 at Claim 7 ("7. The system of claim 6, wherein said processor determines whether to forward said response resource by: searching said first response resource for a list of key terms; and querying said database to determine whether to forward said first response resource to said user, said query based on said search and said user identification code.") Apple 1004.0010 ("On the other hand, if the response is a resource with a field specifying a new URL, 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.")
(d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.

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 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."); *see also* Apple 1004.0009-10; Apple 1010 ¶¶ 57-58. Apple 1002 at Claim 6 ("6. A public network resource access system comprising . . . 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;"); *see also* Apple 1004.0009.

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.
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."); *see also* Apple 1004.0009-10; Apple 1010 ¶¶ 61-62. Apple 1002 at Claim 6 ("6. A public network resource access system comprising . . . 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;"); *see also* Apple 1004.0009. Apple 1002 at Claim 7 ("7. The system of claim 6, wherein said processor determines whether to forward said response resource by: searching said first response resource for a list of key terms; and querying said database to determine whether to forward said first response resource to said user, said query based on said search and said user identification code."); *see also* Apple 1004.0009.

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."); *see also* Apple 1004.0007.

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.
Apple 1002 at 1:29-32 ("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.") (emphasis added). 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.***") (emphasis added) Apple 1004.0009 ("The following discussion is written as if the filter and client are separate programs; however, these methods also work if the ***filter is part of the client***.") (emphasis added); Apple 1010 ¶¶ 63-66.

Claims 15 and 23 have essentially the same scope as Claim 1 except that Claim 1 is directed to outgoing messages, Claim 23 is directed to incoming messages, and Claim 15 does not specify a direction. Because Claim 15 is broader than Claim 1, it is anticipated for the same reasons discussed above for Claim 1. Claim 23 is anticipated for the same reasons discussed above with respect to Claim 1 and for the additional reason that Baker '645 discloses that the same filtering operation may be applied on either outgoing or incoming messages. Apple 1010 ¶¶ 67-69. For example, Baker

'645 discloses that both requested URLs and responses from remote servers are considered for filtering:

> 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***.

Apple 1002 at 3:24-35 (emphasis added). This disclosure is supported in the Provisional application. *See, e.g.*, Apple 1004.0009 ("Our 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, Baker '645 anticipates Claims 1, 2, 9, 15, and 23. Apple 1010 ¶¶ 67-69.

B. Claims 1, 2, And 15 Are Anticipated By U.S. Patent No. 5,696,898 ("Baker '898"), And Claims 9 And 23 Are Rendered Obvious By Baker '898 Alone Or In Combination With Baker '645

Baker '898 (attached as Apple 1003) was filed on June 6, 1995, issued on December 9, 1997, and shares an inventor with Baker '645. Baker '898 qualifies as prior art at least under 35 U.S.C. § 102(e) and was not of record during prosecution of

the '033 Patent. Baker '898 addresses the same problem the '033 Patent purports to address:

> The present invention overcomes the deficiencies of prior schemes 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. 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.

Apple 1003 at 2:65-3:16; Apple 1010 ¶ 71. Baker '898 describes using a "relational database" which "specifies the particular URLs that may be transmitted from a given user terminal to access network resources." Apple 1003 at 3:62-64. Requests may be immediately and unconditionally allowed if they are directed to a URL matching an allow filter:

> 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.

Id. at 4:11-20. Filters may specify particular URLs to unconditionally allow or to unconditionally block:

> 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***.

Id. at 4:27-34 (emphasis added); Apple 1010 ¶ 72. And to provide greater flexibility, Baker '898 discloses that deferred filtering can be achieved by configuring filters to match regular expressions within the messages so that only certain portions of a resource can be accessed while others are blocked:

> More generally, the URL http://ourschool.edu/history/* is a regular expression that specifies all resources within the directory http://ourschool.edu/history or its tree of subdirectories (a resource containing information relevant to a particular school's

> history course). 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.

Apple 1003 at 5:26-47; Apple 1010 ¶¶ 73-74.

Claim 1: Baker '898 anticipates Claim 1, as detailed in the chart below:

1. A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:
Apple 1003 at Abstract ("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. 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."); Apple 1010 ¶ 75.
(a) opening a data stream to send a message through an interface to an Internet server;
Apple 1003 at 1:17-26 ("A user of a computer that is connected to the Internet may cause a program known as a client to request resources that are part of the WWW. Server programs then process the requests to return the specified resources (assuming they are currently available). A standard naming convention has been adopted, known as a Uniform Resource Locator ('URL'). This convention encompasses several types of location names, presently including subclasses such as Hypertext Transport Protocol ('http'), File Transport Protocol ('ftp'), gopher, and Wide Area Information Service ('WAIS').") Inherent. *See* Apple 1001 at 3:18-19; Apple 1010 ¶ 76.
(b) maintaining a database of filtering information comprising a table of filters, said table comprising
Apple 1003 at 3:4-14 ("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."); Apple 1010 ¶¶ 77-78.
(1) filters specifying immediate action, and
Apple 1003 at 4:11-20 ("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."); *Id.* at 3:6-14; Apple 1010 ¶ 79.
(2) filters specifying deferred action;
Apple 1003 at 2:34-38 ("In 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.") *Id.* at 5:30-47 ("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."); Apple 1010 ¶¶ 80-81.
(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
Apple 1003 at 4:11-15 ("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.") 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."); Apple 1010 ¶ 82.
(d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.
Apple 1003 at 4:11-26 ("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. For instance, if URL104 is received by processor 111 from user terminal 107, relational database 114 is accessed. Since URL104 is not one of the URLs associated with user terminal identification code ID107 within relational database 114, processor 111 denies the request for information, and no URL is sent to public network 100.") 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."); Apple 1010 ¶¶ 83-84.

Claim 15: Claim 15 is nearly identical to Claim 1 but broader in that it does not specify whether the filtered message is incoming or outgoing. Claim 15 is anticipated by Baker '898 for the same reasons discussed with respect to Claim 1. Apple 1010 ¶ 88.

Claim 2: Baker '898 also anticipates Claim 2, as detailed in the chart below:

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.
Apple 1003 at 4:11-26 ("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. For instance, if URL104 is received by processor 111 from user terminal 107, relational database 114 is accessed. Since URL104 is not one of the URLs associated with user terminal identification code ID107 within relational database 114, processor 111 denies the request for information, and no URL is sent to public network 100.") 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."); Apple 1010 ¶¶ 85-87.

Claim 23: Baker '898 discusses filtering messages sent from a client to an Internet server (i.e., outgoing messages) by examining the URL sent in the request and

comparing it against a filter database. Baker '898 also states "When 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." Apple 1003 at 1:27-30. Thus, an outgoing message containing a URL may result in an incoming message also containing a URL for another resource or a redirected resource. To the extent the filter of Baker '898 would not inherently also operate on these incoming URLs, it would have been obvious to do so. Baker '898 addresses the problem that "parents or school teachers might wish to have children access useful information, but not obscene material (which the children may be exposed to as a result of innocent exploration of the WWW, or ***through the incidental downloading of a URL***)." *Id.* at 1:37-42 (emphasis added). Thus, Baker '898 specifically contemplates that a request for an "approved" URL might end up incidentally downloading a different (redirected) URL that could include offensive material. Thus, applying the same filtering to URLs returned by a server would ensure that this objective was achieved, and this would have been obvious to a PHOSITA reading Baker '898. Apple 1010 ¶¶ 92. Baker '898 renders Claim 23 obvious.

Alternatively, it would have been obvious to combine the teachings of Baker '645 with Baker '898. These two references share an inventor, Brenda Sue Baker, and Baker '645 explicitly refers to Baker '898:

> In one embodiment, the database or permissions derived from the database are stored local to filter, either on the same machine or

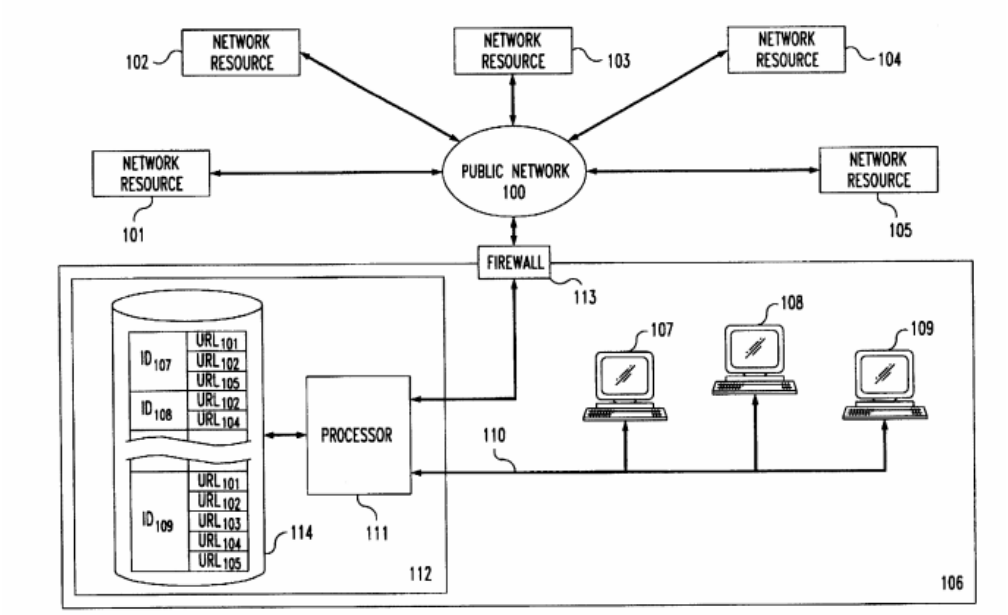
> within a common firewall. Such a system is described in U.S. patent application Ser. No. 08/469,342 [issued as Baker '898]

Apple 1002 at 1:33-36. Baker '645 and Baker '898 are directed to the identical problem of filtering transmissions sent over the Internet, and Baker '645 even directs the reader to consider the specific embodiment disclosed in Baker '898. This explicit invitation to combine would lead a PHOSITA to expect that combining the disclosures to achieve the filter of Baker '898 operating on incoming transmissions was likely to be successful. Apple 1010 ¶ 93. Baker '645 expressly discloses applying filtering operations to incoming URLs returned by Internet servers:

> 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.

Apple 1002 at 5:1-4. The combination of Baker '898 and Baker '645 renders claim 23 obvious.

Claim 9: Claim 9, requiring that the filter be implemented on the client, is rendered obvious by Baker '898. Baker '898 discloses a filter database on a proxy server that maintains separate lists of URL filters—one list for each of the client terminals behind the proxy server. *See* Figure 1 of Baker '898, below, in which database 114 includes filter record ID_{107}—with filter entries URL_{101}, URL_{102}, and URL_{105}—associated with client 107, and filter record ID_{108}—with filter entries URL_{102} and URL_{104}—associated with client 108. *See* Apple 1003 at 3:59-4:26.



Because the filter databases are already divided up to be client-specific, it would be an obvious design choice to locate them on the individual clients (107, 108, 109) to which they apply, as opposed to locating them on a separate proxy server. Apple 1010 ¶¶ 89-90. Indeed, as can be seen from Figure 1, the filters associated with ID_{107} are only applied to messages to and from terminal 107, so it would convenient to locate this filter database on terminal 107 itself. Apple 1010 ¶¶ 89-90. In fact, it was well known at the time that clients on a network could be implemented as "thick clients" or as "thin clients." *Id.* Thin clients include minimal functionality on the client itself and rely on the networked computing power and storage resources to perform most functions. *Id.* Thick clients, on the other hand, are built with more local computing power and storage resources and execute more programs locally. *Id.* Trade-offs such as cost and network speed factor into the decision of whether a network is built with thick or thin clients. *Id.* The decision to locate a filtering

database on the client and perform filtering operations on the client is simply an example of the well-known thin client/thick client design trade-off, and it would have been a natural design choice for a PHOSITA to select between these two known solutions that would have involved ordinary engineering efforts and would not have yielded any unexpected results. *Id.*

In addition, Baker '898 discloses, "[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 . . ." Apple 1003 at 2:34-36 (emphasis added). Baker '898 thus contemplates locating the filter on the client. Baker '898 renders Claim 9 obvious in light of the knowledge of a PHOSITA.

Alternatively, it would have been obvious to combine Baker '898 with the teachings of Baker '645 for the same reasons discussed earlier, including that they are both by the same inventor, are directed to the same subject matter and because Baker '645 explicitly invites the reader to look to Baker '898. Apple 1010 ¶ 91. 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." (emphasis added). Apple 1002 at 1:29-32. Further, referring to Figure 1, which is nearly identical to Baker '898's Figure 1, Baker '645 states, "[h]owever, each ***user terminal*** 107-109 can also include a processor that ***runs filtering code*** for individually controlling access for each terminal." *Id.* at 3:65-67 (emphasis added). *See also* Apple 1004.0009; Apple 1010 ¶ 91. Finally, Baker '645

refers explicitly to Application No. 08/469,342, which became Baker '898, and states that it describes that "the database or permissions derived from the database are stored local to filter, either on the same machine, or within a common firewall." Apple 1002 at 1:33-39. It also states that "the filtering code may be part of a browser, part of a proxy server, or a separate program that determines whether to allow or deny resources." *Id.* at 1:43-45. *See also* Apple 1004.0007; Apple 1010 ¶ 91. A filter that is part of a browser would execute on the client running the browser. The combination of Baker '898 and Baker '645 renders Claim 9 obvious.

C. Claims 1, 2, 15, And 23 Are Anticipated By U.S. Patent No. 5,790,554 ("Pitcher '554").

Pitcher '554 (attached as Apple 1005) was filed on October 4, 1995 and issued on August 4, 1998. Pitcher '554 qualifies as prior art to the '033 Patent at least under 35 U.S.C. § 102(e). Pitcher '554 was not of record during prosecution of the '033 Patent.

Pitcher '554 discloses an improved Internet filtering system that enables filtering based on (1) address information and (2) matching other content in the data packets. Apple 1005 at 3:50-53. Pitcher '554 notes, for example, that prior art systems allow a user to "configure and then apply to a particular port an access list that forwards or drops data packets having a value of 129.1.1.1 in the IP header of the data packet." *Id.* at 3:6-9. In other words, performing "immediate action" filtering to

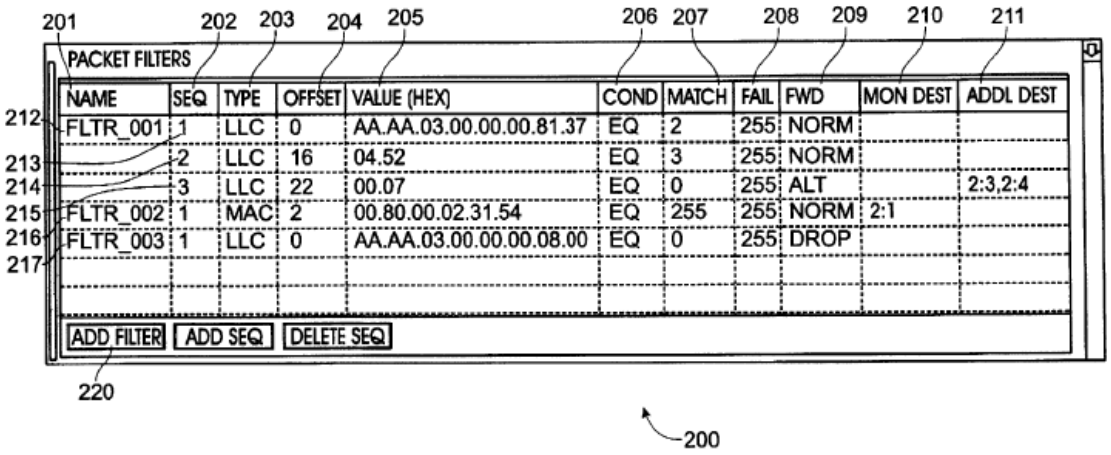
block or allow an Internet Protocol message based on its address was well known in the art.

The system of Pitcher '554 adds the additional capability of blocking or allowing messages based on matching a pattern other than a port or address within the message contents. For example:

> 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.

Id. at 3:53-65. Apple 1010 ¶ 94-95. To implement such filters, Pitcher '554 discloses building a table of filters, such as the one depicted in Figure 2 of the reference and reproduced below:

Fig. 2



The filter table shown in Figure 2 has a flexible structure. The first filter, "FLTR_001," has three parts, identified by sequence numbers 1, 2, and 3, as shown in the "SEQ" column (202). *Id.* at 6:66-7:9. The "EQ" in the COND (206) column specifies that the first filter of FLTR_001 looks to match a pattern in the incoming (or outgoing) packet at OFFSET 0 with the VALUE "AA.AA.03.00.00.00.81.37." *Id.* In the case of a MATCH (207), the algorithm proceeds to subfilter "2" of FLTR_001, which would check for an additional pattern match at OFFSET 16. In the case of a FAIL (208), the "255" indicates that the FLTR_001 would exit at that point (i.e., would not proceed to subfilters 2 and 3). *Id.* at 8:33-63. The "FWD" column (209) indicates whether the message should be forwarded to the intended destination (NORM), sent to a different address (ALT), or blocked (DROP) in the case that the match condition is true. *Id.* at 9:5-20. FLTR_001 is a "deferred action" filter. Apple 1010 ¶¶ 103-04. FLTR_002 (216), on the other hand, is a 1-stage filter that applies the specified action to any message matching MAC address "00.80.00.02.31.54."

"The filter forwards all packets destined to a device having a MAC address of 00800023154(hex) to a monitoring device or analyzer attached to module 2, port 1, in addition to the normal destination port." *Id.* at 7:12-15. Alternatively, the command in the "FWD" column for FLTR_002 could be set to "DROP," in which case, any messages destined for the device at that MAC address would be unconditionally dropped. Thus, FLTR_002 is a "immediate action" filter in the context of the '033 Patent because it blocks or allows messages directed to a particular network address, in this case, a hardware MAC address. Apple 1010 ¶¶ 99-103.

Thus, as shown in the filter table, Pitcher '554 specifies "immediate" filters (such as FLTR_002), which can block (DROP) or allow (NORM) packets that match a particular address on a network. The filter table also specifies "deferred" filters, such as FLTR_001, which can perform multi-stage pattern matching functions on an incoming or outgoing message to decide whether to block (drop) it or allow it to continue to its intended destination based on matching keywords or patterns in content other than the network address or port. Apple 1010 ¶¶ 99-103.

Claim 1: The claim chart below demonstrates that Pitcher '554 anticipates Claim 1:

1. A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:
Apple 1005 at 3:48-53 ("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.") Apple 1005 at Abstract ("A method and apparatus for filtering data packets from a

network device, such as a LAN switch, onto a network coupled thereto based on the content of the data packets.")
Apple 1005 at 3:4-9 ("For example, to filter on an Internet protocol (IP) data packet with an IP address of 129.1.1.1, a user may configure and then apply to a particular port an access list that forwards or drops data packets having a value of 129.1.1.1 in the IP header of the data packet."); Apple 1010 ¶ 97.

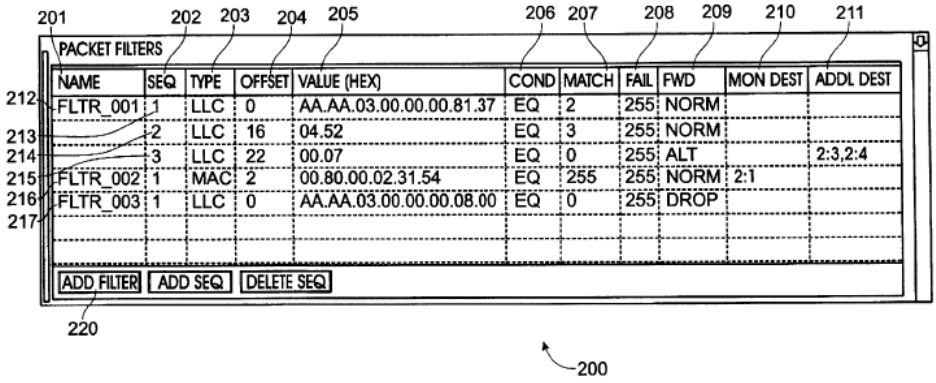
(a) opening a data stream to send a message through an interface to an Internet server;

Apple 1005 at 6:26-33 ("In general, a packet filter directs a network device to forward certain packets to a specified set of destination ports or to drop the packet, i.e., discard the packet. Filtering may be used to limit the ports from which broadcast packets are sent, control access to network segments and devices, redirect traffic to ports in addition to or rather than the normal destination port(s).")
Further, the '033 Patent admits that opening a data stream is an inherent part of the existing Internet Protocol for sending messages over a network. *See* Apple 1001 at 3:18-19.
Apple 1005 at 6:1-7 ("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."); Apple 1010 ¶ 98.

(b) maintaining a database of filtering information comprising a table of filters, said table comprising

Apple 1005 at Fig. 2:

Fig. 2



Apple 1005 at 6:66-7:9 ("In FIG. 2, window 200 displays three filter groups. Each filter group has a name 201. As will be seen, filter group 212 is named FLTR-- 001, and redirects all Novell NetWare printer requests to the specific token ring LAN segment to which the printers are attached. The filter group is comprised of three filters. Each filter has, and is identified by, a unique sequence number 202. Filter 213 has a sequence number of 1, filter 214 has a sequence number of 2, and filter 215 has

a sequence number of 3. Filter 213 checks for IPX packets, filter 214 checks for IPX SAp packets, and filter 215 checks for printer requests."); Apple 1010 ¶¶ 99-100.
(1) filters specifying immediate action, and
Apple 1005 at 7:10-16 ("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.") Apple 1005 at 3:4-9 ("For example, to filter on an Internet protocol (IP) data packet with an IP address of 129.1.1.1, a user may configure and then apply to a particular port an access list that forwards or drops data packets having a value of 129.1.1.1 in the IP header of the data packet."); Apple 1010 ¶¶ 101-102.
(2) filters specifying deferred action;
Apple 1005 at 8:4-32 ("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."); Apple 1010 ¶¶ 103-104.
(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
Apple 1005 at 9:5-19 ("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)."); Apple 1010 ¶ 105.
(d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.
Apple 1005 at 3:49-4:4 ("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. 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. (It should be noted that the normal destination port or ports may be determined by standard forwarding rules, for example, transparent or source route bridging rules, routing rules, or proprietary forwarding rules). The next filter may define a different forwarding action for data packets that do not meet the condition specified by the present filter."); Apple 1010 ¶¶ 106-07.

Claim 15: Claim 15 is nearly identical to Claim 1 but broader in that it does not specify whether the filtered message is incoming or outgoing. Claim 15 is anticipated by Pitcher '554 for the same reasons discussed with respect to Claim 1. Apple 1010 ¶¶ 112-14.

Claim 23: Claim 23 differs from Claim 1 only in that it claims filters that operate on incoming messages, as opposed to outgoing messages. The filters

disclosed in Pitcher '554 operate on both outgoing and incoming messages. For example, Pitcher '554 states the following:

> 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.

Apple 1005 at 3:53-65 (emphasis added). For this reason, and for the same reasons discussed with respect to Claim 1, Pitcher '554 anticipates Claim 23. Apple 1010 ¶¶ 112-14.

Pitcher '554 anticipates Claim 2, as shown in detail in the table below:

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.
Apple 1005 at 9:5-19 (emphasis added) ("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).”); Apple 1010 ¶¶ 110-11 (emphasis added).

Thus, Pitcher ’554 anticipates Claims 1, 2, 15, and 23.

D. Claim 9 Is Obvious In View Of Pitcher ’554 Alone Or In Combination With Baker ’645.

Pitcher ’554 discloses that the filtering operations are performed on a local area network (LAN) switch and indicates that the filtering could also be implemented on other network 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.” Apple 1005 at 5:8-12; Apple 1010 ¶¶115-16. Pitcher ’554 further discloses that the strategy of dividing a network into LANs to conserve bandwidth culminates in a LAN with just a single workstation:

> 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.

Apple 1005 at 1:27-34. As in this example, when the filtering operations carried out on the LAN switch are for the benefit of a single workstation (client), it would be

more efficient to simply implement the filtering on the client workstation itself. Apple 1010 ¶¶ 116-18. Doing so would eliminate unnecessary hardware because instead of installing a separate gateway or switch whose only function was to allow or block network messages to and from a single client computer, that gateway could be implemented on the client itself, since all of the functionality of that single gateway was already dedicated to the single client. It would have been obvious to a PHOSITA to perform the filtering operations discussed in Pitcher '554 on the client workstation computer. Indeed, it would have been a matter of design choice to configure a client workstation as a thick client or thin client, as Dr. Knutson discusses. Apple 1010 ¶¶ 116-18. Thus, Pitcher '554, in combination with the knowledge of a PHOSITA, renders Claim 9 obvious.

Baker '645

Alternatively, it would have been obvious to a PHOSITA to combine Pitcher '554 with Baker '645. Baker '645 discloses an Internet filtering system with the capability of filtering based on content ratings as well as keywords and IP address information. *See, e.g.,* Apple 1002 at 4:21-27; 5:26-30. A PHOSITA would have been motivated to combine the teachings of Pitcher '554 with the teachings of Baker '645 to filter based on content ratings in order to achieve a more capable and flexible filtering system. Apple 1010 ¶¶ 119-20. Because Baker '645 discloses that the filter itself can be implemented either on the client computer or on a separate machine,

such as a proxy server, a PHOSITA would have recognized that the location of the filter is matter of design choice:

> 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). Similarly, Baker '645 discloses:

> 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.***"

Apple 1002 at 3:62-67. It would have been obvious to a PHOSITA, in light of Baker '645, to implement the filters disclosed in Pitcher '554 on the client machine, because this was simply one of the design choices facing a PHOSITA—whether to implement a thin or thick client—during the design process. Apple 1010 ¶¶ 119-20. The combination of Pitcher '554 and Baker '645 renders obvious Claim 9 of the '033 Patent.

E. Claims 1, 2, 9, 15, And 23 Are Anticipated By U.S. Patent No. 5,706,507 ("Schloss '507")

Schloss '507 was filed on July 5, 1995 and issued on June 6, 1998 and qualifies as prior art to the '033 Patent under at least 35 U.S.C. § 102(e). Schloss '507 was not before the Office during prosecution of the '033 Patent and is attached hereto as

Apple 1006. Schloss '507 discloses a system for controlling access to resources on the Internet. *See, e.g.,* Apple 1006 at Abstract:

> 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.

Schloss '507 explains that when a user requests a resource located at a first URL, he or she may be presented with a page containing links to additional URLs that may or may not be appropriate for viewing. Apple 1006 at 6:23-36. Thus, two types of filters can be configured: "AdviseOnURL" filters and "AdviseOnURLIncludingLinks" filters. *Id.* at 6:17-19; Apple 1010 ¶¶ 121-23. An "AdviseOnURL" filter simply blocks or allows access to the "particular page of content data requested from the content server 6" (Apple 1006 at 6:20-22) and operates as an "immediate filter" to control access based on the network address. An "AdviseOnURLIncludingLinks" filter examines the content returned by the original URL so that any links embedded in that page can be evaluated as well. *Id.* at 6:23-28 ("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.") This second type of filter is a "deferred action" filter because it examines the content of the retrieved data to block access to a resource, for example, that might otherwise have been allowed based solely on its network address. Apple 1010 ¶¶ 121-23. Specifically, Schloss '507 states:

> In step 715, the advisory server 20 compares the URL field 303 of the AdviseOnURLIncludingLinks signal with the entries stored in the advisories knowledge base 22 to determine if one or more matching entries are present.

Apple 1006 at 7:36-40. Schloss '507 discloses that in some embodiments, the filter may be implemented on the client computer, while in others, it may be implemented on a proxy server:

> As described above, the invention is embodied in a client running a Web Browser adapted to communicate with one or more advisory servers. According to a second embodiment of the present invention, certain inventive aspects of the client running a Web Browser may be embodied in a proxy server.

Apple 1006 at 11:56-61. Further, the client computer may generate and maintain filter database information by using characterization data sent by a content server:

> 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.

Id. at 5:2-7. Thus, the filtering operations disclosed by Schloss '507 may be carried out on a client device, either by querying a content server or by downloading the characterization data and generating its own local filtering information from that data. Apple 1010 ¶¶ 121-23. Schloss '507 thus anticipates or renders obvious Claims 1, 2, 9, 15, and 23, as shown in the charts below:

1. A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:
Apple 1006 at Abstract ("The invention comprises an advisory server operated by, for example, a third party watchdog group, which rates the content of data downloaded from a content server to a client in order to block or censor unwanted material. 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."); Apple 1010 ¶ 125.
(a) opening a data stream to send a message through an interface to an Internet server;
Apple 1006 at 4:30-36 ("More specifically, a client system running a Web Browser request 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."); Apple 1010 ¶ 126.
(b) maintaining a database of filtering information comprising a table of filters, said table comprising
Apple 1006 at 4:57-5:7("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."); Apple 1010 ¶¶ 127-28.
(1) filters specifying immediate action, and
Apple 10006 at 6:12-23 ("FIG. 5(A) illustrates a format of the advisory request signal transmitted by the client 25 running a Web Browser to the advisory server 20 according to the present invention. As shown, the advisory request signal includes a header field 301 and a URL field 303. The header field 301 includes a command verb that identifies the type of request. For example, the command verb may be "AdviseOnURL" or "AdviseOnURLIncludingLinks". 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 1010 ¶ 129.
(2) filters specifying deferred action;
Apple 1006 at 6:23-32 ("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 7:36-44 ("In step 715, the advisory server 20 compares the URL field 303 of the AdviseOnURLIncludingLinks signal with the entries stored in the advisories knowledge base 22 to determine if one or more matching entries are present. An exact match to the URL field 303 may be required. In the alternative a fuzzy match may be utilized wherein if an exact match is not found, the entry having the longest matching prefix will be considered a match."); Apple 1010 ¶¶ 130-31.
(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
Apple 1006 at 5:59-6:6 ("Referring now to FIG. 3b, in step 255 the client may inhibit loading of or load the content data associated the contour request as a function of the received characterization data. For example, if the characterization data indicates the advisory server 20 has no relevant information related to the requested content data, the client 25 may load the content data associated with the content request; yet, if 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. In step 260, the client 25 may generate additional information related to the content request. The addition information may be an additional content request or any other meta-data related to, or contrasted with, the requested content data. In step 265, the client 25 may display the additional information to the user."); Apple 1010 ¶¶ 132.
(d) determining whether to prevent or allow the outgoing transmission of the message

based on the comparison.
Apple 1006 at 5:59-6:6 ("Referring now to FIG. 3b, in step 255 the client may inhibit loading of or load the content data associated the contour request as a function of the received characterization data. For example, if the characterization data indicates the advisory server 20 has no relevant information related to the requested content data, the client 25 may load the content data associated with the content request; yet, if 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. In step 260, the client 25 may generate additional information related to the content request. The addition information may be an additional content request or any other meta-data related to, or contrasted with, the requested content data. In step 265, the client 25 may display the additional information to the user."); Apple 1010 ¶¶ 133-34.

Claim 2: Schloss '507 discloses that access to particular resources may be blocked or allowed depending on the rating returned by an advisory server: "[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. The "client's selected preferences" specify that some messages should be sent while others should be blocked. Apple 1010 ¶¶ 135-36.

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.
Apple 1006 at Abstract ("The 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 5:59-6:6 ("Referring now to FIG. 3b, in step 255 the client may inhibit loading of or load the content data associated the contour request as a function of the received characterization data. For example, if the characterization data indicates the advisory server 20 has no relevant information related to the requested content data, the client 25 may load the content data associated with the content request; yet, if 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. In step 260, the client 25 may generate additional information related to the content request. The addition

information may be an additional content request or any other meta-data related to, or contrasted with, the requested content data. In step 265, the client 25 may display the additional information to the user.") Apple 1010 ¶¶ 135-36.

Claim 9: The filtering steps are performed on the client: "[t]he 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. *See also id.* at 11:56-58 ("As described above, the invention is ***embodied in a client*** running a Web Browser adapted to communicate with one or more advisory servers." (emphasis added)). To the extent certain filtering information is maintained in an advisory server, Schloss '507 discloses that it is also possible to 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; Apple 1010 ¶ 137. To the extent claim 9 is not anticipated by this disclosure, it is rendered obvious. Because Schloss '507 discloses that filtering is performed on the client and that the client can generate additional information based on downloaded characterization data, it would have been a simple matter of design choice to locate all of the filtering data on the client, as well. Schloss '507 renders Claim 9 obvious, if not anticipated. Apple 1010 ¶ 137.

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.

Apple 1006 at 5:2-7("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.")
Apple 1006 at 11:56-61 ("As described above, the invention is embodied in a client running a Web Browser adapted to communicate with one or more advisory servers. According to a second embodiment of the present invention, certain inventive aspects of the client running a Web Browser may be embodied in a proxy server."); Apple 1010 ¶ 137.

Claims 15 and 23: Schloss '507 discloses that outgoing requests are filtered, as described above. *See, e.g.,* Apple 1006 at 6:12-36 (discussing "AdviseOnURL" requests). 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 6:27-28. Schloss '507 therefore discloses applying filters to both outgoing and incoming messages. Schloss '507 anticipates Claims 15 and 23 for the same reasons it anticipates Claim 1. Apple 1010 ¶¶ 138-39.

VII. CONCLUSION

Each of the grounds for invalidity presented above is non-cumulative and reasonably likely to prevail. *Inter Partes* Review of the '033 Patent on each of the grounds presented should be instituted.

Respectfully Submitted,

/s/ Mark E. Miller
Mark E. Miller (Reg. No. 31401)

CERTIFICATE OF SERVICE

I hereby certify that on March 30, 2015, I caused a true and correct copy of the foregoing materials:

- Petition for *Inter Partes* Review of U.S. Patent No. 5,884,033 Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104
- Exhibits 1001-1011 of Petition for *Inter Partes* Review of U.S. Patent No. 5,884,033

to be served via Express Mail or an equivalent service on the following attorney of record as listed on PAIR:

Eric Andersland
Schwegman Lundberg & Woessner/Open TV
P.O. BOX 2938
Minneapolis, MN 55402-0938

A courtesy copy was also sent to the patent owner's litigation counsel at the following address:

Robert F. McCauley; Jacob A. Schroeder; Gerald F. Ivey;
Smith R. Brittingham IV; Elizabeth A. Niemeyer; John M. Williamson;
Aliza A. George; Robert D. Wells; Stephen E. Kabakoff
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
3300 Hillview Avenue
Palo Alto, CA 94304-1203

/s/ Xin-Yi Zhou
Xin-Yi Zhou (Reg. No. 63366)