Filed on behalf of Unified Patents Inc.
By: Scott A. McKeown, Reg. No. 42,866
Victor Cheung, Reg. No. 66,229
OBLON, MCCLELLAND, MAIER & NEUSTADT, L.L.P.
1940 Duke Street
Alexandria, VA 22314
Tel: (703) 413-3000
Email: cpdocketmckeown@oblon.com

Roshan S. Mansinghani, Reg. No. 62,429
Jonathan Stroud, Reg. No. 72,518
Unified Patents Inc.
1875 Connecticut Ave. NW, Floor 10
Washington, D.C., 20009
Tel: (214) 945-0200
Email: roshan@unifiedpatents.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Unified Patents Inc.,
Petitioner

v.

Catonian IP Management LLC
Patent Owner

IPR2017-_____
U.S. Patent No. 8,799,468

PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1-5, 9, 11-13, 19, 23-27, AND 32-34 OF U.S. PATENT NO. 8,799,468 UNDER 35 U.S.C. §§311-319

TABLE OF CONTENTS

EXHIBIT LIST

Exhibit	Description
1001	U.S. Patent No. 8,799,468 to Burke, II et al.
1002	Andrew S. Tanenbaum, "Computer Networks," Prentice-Hall, Inc. 3rd ed., 1996, pp. 4-8, 50-56, 408-413
1003	Declaration of Norman Hutchinson, Ph.D.
1004	U.S. Patent No. 5,987,611 to Freund
1005	U.S. Patent Application No. US 2002/0032870 to Spusta et al.
1006	Norbert Pohlmann et al., "Firewall Architecture for the Enterprise," Wiley Publishing, Inc. 2002, pp. 114-135, 149-155, 174-181, 308-315
1007	Webster's New World Dictionary of American English (3rd ed., 1988)
1008	Prosecution History of Application No. 13/369,174, resulting in U.S. Patent No. 8,799,468
1009	U.S. Patent No. 5,987,606 to Cirasole et al.
1010	Declaration of Scott Bennett, Ph.D.
1011	U.S. Patent No. 8,122,128 to Burke, II et al.
1012	U.S. Provisional Patent Application No. 60/523,057
1013	U.S. Provisional Patent Application No. 60/538,370
1014	U.S. Provisional Patent Application No. 60/563,064

I. INTRODUCTION

Pursuant to 35 U.S.C. §§311-319, Unified Patents Inc., ("Unified" or "Petitioner") petitions the PTAB to institute *inter partes* review of claims 1-5, 9, 11-13, 19, 23-27, and 32-34 of U.S. Patent No. 8,799,468 to Burke, II et al. ("the '468 Patent," EX1001).

The '468 Patent claims that regulating network access by using a centralized controller is new. It is not. Regulating network access has been around since the advent of networks themselves, and virtually every different architecture for doing so has been used, including using a centralized controller. ***None*** of the devices claimed in the '468 Patent are new, ***nor*** is their combined presence in the same network system new, ***nor*** is their specific usage to regulate network access new. As the prior art discussed in this Petition shows, the challenged claims recite nothing more than well-known, network-access regulation using a well-known architecture.

II. MANDATORY NOTICES

Pursuant to 37 C.F.R. §42.8(a)(1), Petitioner provides the following mandatory disclosures:

A. Real Party-in-Interest

Pursuant to 37 C.F.R. §42.8(b)(1), Petitioner certifies that Unified is the real party-in-interest.

B. The Patent Owner

The ’468 Patent is assigned to Catonian IP Management, LLC (“Catonian”).

C. Related Matters

The ’468 Patent has been asserted in the following now-closed litigations, none of which involve Unified:

1. *Catonian IP Management, LLC v. Charter Communications, Inc. et al.*, Case No. 2:17-cv-00191 (E.D. Tex. March 10, 2017); and
2. *Catonian IP Management, LLC v. Cequel Communications, LLC et al.*, Case No. 2:17-cv-00190 (E.D. Tex. March 10, 2017).

D. Identification of Lead and Back-Up Counsel

Pursuant to 37 C.F.R. §42.8(b)(3), Petitioner provides the following designation of counsel: lead counsel is Scott A. McKeown (Reg. No. 42,866), primary back-up counsel is Roshan S. Mansinghani (Reg. No. 62,429), and other back-up counsel are Victor Cheung (Reg. No. 66,229) and Jonathan Stroud (Reg. No. 72,518).

E. Service Information

Pursuant to 37 C.F.R. §42.8(b)(4), papers concerning this matter should be served on the following:

Address:	Scott A. McKeown Oblon LLP 1940 Duke Street Alexandria, VA 22314
Email:	cpdocketmckeown@oblon.com
Telephone:	703-413-3000
Fax:	703-413-2220

Address:	Jonathan Stroud, Chief Patent Counsel Unified Patents Inc. 1875 Connecticut Ave. NW, Floor 10 Washington, D.C. 20009
Email:	jonathan@unifiedpatents.com
Telephone:	202-805-8931
Fax:	650-887-0349

Petitioner consents to service via email to cpdocketmckeown@oblon.com and roshan@unifiedpatents.com.

III. PAYMENT OF FEES

The undersigned authorizes the Office to charge the required fees and any additional fees that might be due to Deposit Account No. 15-0030.

IV. REQUIREMENTS FOR *INTER PARTES* REVIEW

As set forth below and pursuant to 37 C.F.R. §42.104, each requirement for *inter partes* review of the '468 Patent is satisfied.

A. Grounds for Standing

Petitioner certifies pursuant to 37 C.F.R. §42.104(a) that the '468 Patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review challenging the patent claims on the grounds identified herein.

B. Identification of Challenge Under 37 C.F.R. §42.104(b)

Petitioner requests *inter partes* review and cancellation of '468 Patent claims 1-5, 9, 11-13, 19, 23-27, and 32-34 as being obvious under 35 U.S.C. §103. The '468 Patent is a continuation of Application No. 10/989,023, now U.S. Patent No. 8,122,128 (EX1011), filed on November 16, 2004 and also claims priority to three provisional applications (EX1012-EX1014), the earliest filed on November 18, 2003. (EX1001).

1. The Specific Art on which the Challenge is Based

Petitioner relies upon the following patent and published application, neither of which was considered by the examiner during the '468 Patent's prosecution:

EX1004 – Issued on November 16, 1999, U.S. Patent No. 5,987,611 ("*Freund*") is prior art under 35 U.S.C. §102(b).

EX1005 – Published on March 14, 2002, U.S. Patent Application Publication No. US 2002/0032870 ("*Spusta*") is prior art under 35 U.S.C. §102(b).

2. The Specific Grounds on which the Challenge is Based

Petitioner respectfully requests cancellation of claims 1-5, 9, 11-13, 19, 23-27, and 32-34 based on the following grounds:[1]

[1] Grounds 1 and 2 are each single reference obviousness rejections under 35 U.S.C. §103(a). As discussed in below, *Freund* and *Spusta* teach all the features in the respective claims of the '468 Patent. Depending on claim interpretation, one might argue that some features are not explicitly disclosed as being present in the same individual embodiment(s). (*See Net MoneyIn, Inc. v. Verisign, Inc.*, 545 F.3d 1359, 1368-71 (Fed. Cir. 2008).) For example, components in both Figs. 3A and 3B of *Freund* are relied on in Ground 1, but the configurations in those figures are described as being modifications of one another. (EX1004, 21:57-59). Based on *Freund's* own disclosure, a person of ordinary skill in the art ("POSA") would have understood that Figs. 3A and 3B are obvious variants of each other, despite being "alternative" embodiments. Therefore, *Freund* and *Spusta*, individually, teach all features claimed by the '468 Patent, which would have been obvious to a POSA when considering either *Freund* or *Spusta* as a whole, respectively, as discussed in the grounds of unpatentability below.

#	Claims	35 U.S.C. §	Prior Art
1	1-5, 9, 12, 19, 23-27, 33	103(a)	*Freund*
2	1-3, 11, 13, 23-25, 32, 34	103(a)	*Spusta*

V. DECLARATION EVIDENCE

This Petition is supported by the declaration of Professor Norman Hutchinson, Ph.D., a Computer Science professor at the University of British Columbia with over twenty-five years of experience in distributed systems, having written and lectured extensively on this topic. *See* EX1003. Dr. Hutchinson performed a thorough analysis of the skill level of a POSA, EX1003, ¶¶18-21, the content and state of the prior art, *id*., ¶¶31-51, claim construction, *id*., ¶¶52-70, and the teachings and suggestions that a POSA would have understood based on the prior art, *id*., ¶¶71-198, including a thorough element-by-element analysis of the asserted prior art.

VI. U.S. PATENT 8,799,468

A. Summary

The ’468 Patent is concerned with a concept that was already old as of 2003: regulating Internet access. It simply seeks to prevent users from accessing content

(such as Internet sites) by using a centralized controller. (EX1001, Abstract). The controller (the "internet control point" or "ICP) sends instructions to various gateway units ("communication gateways" or "CGs") to provide access restrictions on users at subscriber terminals associated those gateway units. When the user requests access to a web site, the request is evaluated by the gateway unit, and access is granted or denied based on the instructions from the controller. (EX1001, 2:23-38, 3:34-4:48).

As shown in the flow chart of Fig. 5 below, the alleged invention of the '468 Patent can be distilled into as little as four steps, most of which describe trivial steps of requesting and sending data:

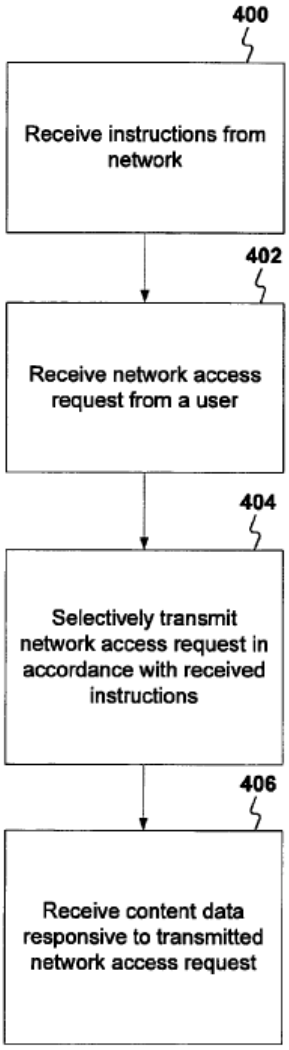


Figure 5

Similarly, claim 1 of the '468 Patent is directed to these broad functions: "generat[ing] controller instructions," "transmit[ting] the controller instructions," receiv[ing] the controller instructions," "receiv[ing] user-entered content requests," "selectively transmit[ting] the content requests … in accordance with the controller instructions," and "transfer[ring] received content data." (EX1001, 18:30-54.) The remainder of the claim describes the system's architecture that performs the above

functions, but these, too, describe basic network elements and functions (i.e., a user interface, processors, network interfaces).

Annotated Fig. 1 of the '468 Patent, below, shows this basic system structure, in which users are connected to communication gateways (in orange), and an internet control point (in red) communicates with the communication gateways over a network (in yellow).

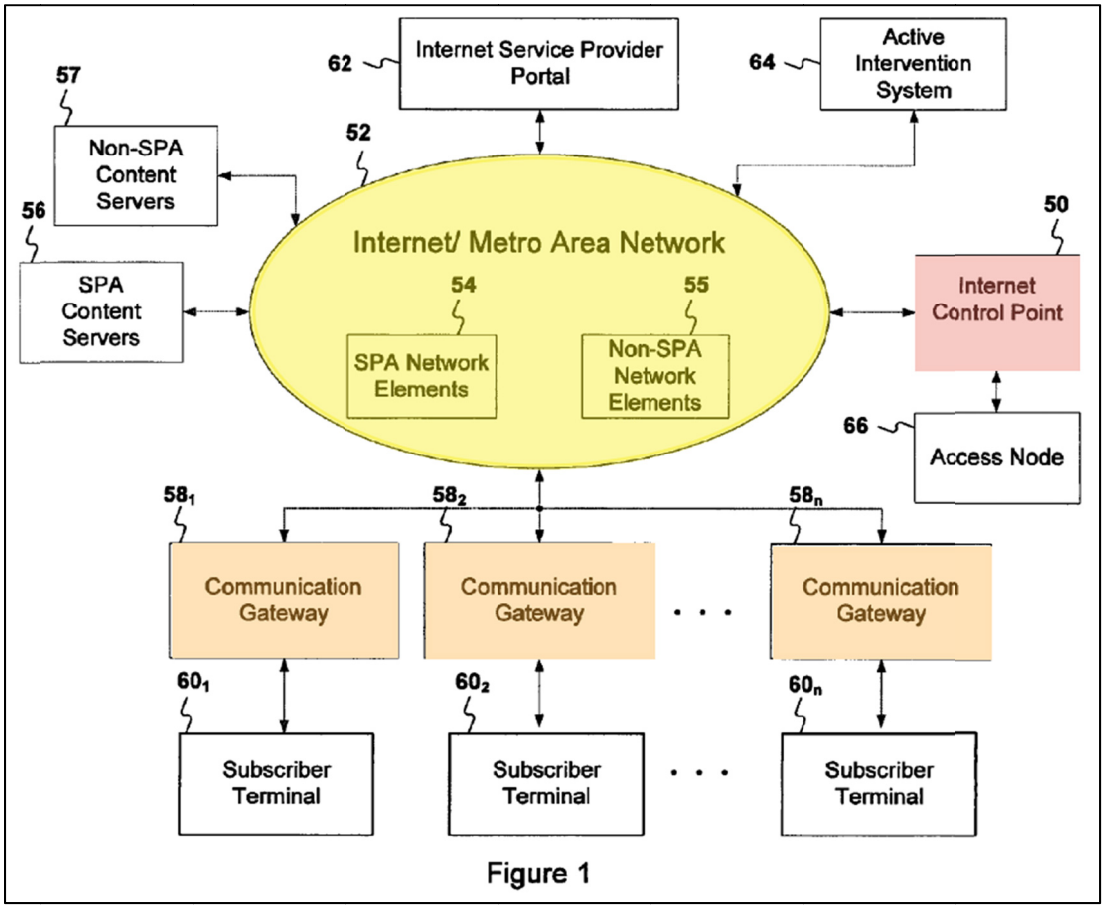


Figure 1

To ensure each gateway unit has up-to-date access instructions, both the controller and the gateway units have databases that store access instructions, and the controller sends new database entries to the gateway units. (EX1001, 6:15-18).

Database entries may include, for example, blocked or permitted URLs or IP addresses. (EX1001, 16:15-50). *See also* EX1003, ¶¶22-25.

As seen above, the alleged invention of the '468 Patent is no more than a collection of network-connected computing elements, in which one computing element instructs another computing element to regulate access to certain content. But, the regulation of access through issuing instructions is an old and well-known technique. As will be discussed throughout this Petition, others in the field had already used the alleged invention of the '468 Patent well prior to the date in question.

B. Prosecution History

Issued on August 5, 2014, the '468 Patent had a short prosecution history, with the examiner considering less than a dozen references. (EX1008; EX1001, p. 1). The examiner issued a restriction requirement and a single office action that rejected the claims on double patenting, anticipation, and obviousness grounds. (*See* EX1008, pp. 141-144 and 164-180). In responding to the prior art rejections, the applicants distinguished over the primary reference, Gregg, by arguing: "it is submitted that Gregg does not teach the recited 'controller node,' 'controller instructions,' and 'gateway units,' and the relationships between them, i.e., the 'controller node' generating the 'controller instructions,' and transmitting the 'controller instructions' to the 'gateway units,' for the 'gateway units' to use to

'selectively transmit content requests to the service provider network.'" (EX1008, p. 205). On June 3, 2014, the examiner allowed the claims, stating only generally that the prior art did not teach or render obvious every element recited in the independent claims. (*See* EX1008, pp. 221-227).

Therefore, one can infer that the examiner believed the alleged point of novelty was in the particular claimed network architecture (i.e., gateway units and a controller) and their interactions (i.e., the controller sends instructions to the gateway units for regulating network access). The prior art references discussed below, which were not before the examiner, show that this architecture and the interactions between the various components were well known, rendering each of the challenged claims unpatentable.

C. Background of the Technology

Regulating user access in a networked computer system was well-known and well-published prior to 2003. For example, several books were published prior to 2003 that explain, in great detail, the need for network security and how to implement such security protocols. (EX1003, ¶¶31-47).

Additionally, prior to 2003, a POSA would have understood that regulating access to information on the Internet could take a number of available forms based on the needs of the engineer designing the system. U.S. Patent No. 5,987,606, issued on November 16, 1999 to Cirasole et al. ("*Cirasole*"), for example,

describes a number of the possible variants for regulating access to the Internet, otherwise known as content filtering. (EX1009). These include exclusive filtering, or black-listing, which prevents access to all sites on a predetermined list of Internet sites and inclusive filtering, or white-listing, which allows access only to a predetermined list of Internet sites. (EX1009, 1:44-48; EX1003, ¶34).

Cirasole also describes that there are a number of locations in the network where the filtering can be performed: (1) on the local (client) machine (EX1009, 1:58-2:12); (2) on a local server, just like the '468 Patent (EX1009, 2:13-35); and (3) on the server that stores the content (EX1009, 2:36-45). *Cirasole* makes it clear that these various options were all well within the skill set of a POSA before 2003, and that such a person would have readily pursued any one of those architectures depending on their specific design goals. (EX1009, 1:15-2:49; EX1003, ¶35). Thus, content filtering and the various architectures to perform this functionality–including the '468 Patent's architecture–were well known before 2003. (EX1003, ¶¶31-47).

VII. PERSON OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art is evidenced by the prior art. *See In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (determining that the Board did not err in adopting the approach that the level of skill in the art was best

determined by references of record). The prior art discussed herein, and in the declaration of Dr. Hutchinson, demonstrates that a POSA, at the time the '468 Patent was filed, would have had a bachelor's degree in Computer Science, or related discipline, and two years of relevant experience and knowledge of regulating network access and designing such systems, TCP/IP-based networking as practiced in the Internet, routers, web proxies, web caches, and web servers, and distributed systems and their advantages and management. (EX1003, ¶21).

VIII. CLAIM CONSTRUCTION (37 C.F.R. §42.104(b)(3))

The '468 Patent has not expired, and thus, its claims should be interpreted according to their broadest reasonable interpretation ("BRI") in view of the specification in which they appear. 37 C.F.R. §42.100(b). Petitioner adopts the plain meaning for all claims terms, unless otherwise discussed below.

A. "service provider network"

All challenged claims recite this term. "Service provider network," as used in the '468 Patent, should be interpreted as "a network over which content is delivered."

The term "service provider network" does not appear in the specification. The specification, however, discusses "service providers," explaining that "service providers [are] for delivering content" and that "[s]ervice providers include…

telephone line carriers, enterprise data centers, and cable television providers." (EX1001, 1:24-37).

For example, the specification discusses service providers delivering content over the Internet, and as such, the Internet serves as one example of a service provider network, as would a LAN. (EX1001, 1:42-2:2; 3:43-46; 4:54-63; 6:54-62).

Accordingly, a POSA would have understood the BRI of "service provider network" to be "a network over which content is delivered." (EX1003, ¶¶53-55).

B. "controller instructions"

All challenged claims recite this term. "Controller instructions," as used in the '468 Patent, should be interpreted as "information that is sent by the controller that is used to direct the actions of a network unit."

The specification does not describe any form of controller instructions, nor does it provide any explicit examples of controller instructions as they would have been implemented in practice. Instead, controller instructions are only described according to their purposes (i.e., what the network units do according to the instructions). (EX1001, 10:7-13; 10:59-63). In the '468 Patent, the "instructions" are from a controller (e.g., an ICP), typically to another network unit (e.g., gateway units or SPA (Service Preference Architecture)-controlled network elements). (EX1001, 3:37-50; 5:19-23). Functionally, the "instructions" are information

primarily used by gateway units to allow or deny access to a network server. (EX1001, 9:55-61). For example, the instructions sent from the controller may include lists of URLs or IP addresses that should be blocked from subscriber access. (*See* EX1001, 8:54-59, 14:39-41, 15:53-18:21).

In this way, the controller instructions may include entries (e.g., URLs and IP addresses) for a rule list to be followed by the gateway units:

> In step 400, **a gateway unit associated with a user receives controller instructions from the network**. Next, at step 402, the gateway unit receives a network access request from a user, via a subscriber terminal. At step 404, **the gateway unit selectively transmits the network access requests over the network in accordance with the controller instructions**.
>
> …
>
> CGs 58, under ICP 50 control, may provide a network-based Digital Rights Management (DRM) service. The DRM service denies subscribers the capability to send or to receive data from or to "pirate" URLs or IP addresses that are known to contain unlicensed copyrighted material. **In implementing this denial, CG 58 deletes the "pirate" URL or IP address and substitutes the URL or IP address of a site that offers licensed copyrighted materials for legal, authorized sale.** The list of "pirate" URLs or IP addresses that are known to contain unlicensed copyrighted material may be regularly updated, similar to the manner in which virus definitions are regularly updated.

…

Upon registration of a CG 58 as "active," **ICP 50 may update the list in CG 58 of DRM URL or IP address substitutions.**

(EX1001, 7:55-8:18, emphasis added).

Accordingly, a POSA would have understood that the BRI of "controller instructions" is "information that is sent by the controller that is used to direct the actions of a network unit." And, as discussed above, the controller instructions may include URLs or IP addresses or a database or list of URLs or IP addresses. (EX1003, ¶¶56-64).

C. "gateway unit"

All challenged claims recite this term. "Gateway unit," as used in the '468 Patent, should be interpreted as "a network component that regulates access to a network."

The specification refers to gateway units as "Communication Gateways (CGs)" (EX1001, 3:39-40) and describes that they perform "packet inspection processing… to determine which data can be allowed to flow through CGs 58 to and from subscriber terminals." (EX1001, 5:26-33).

The '468 Patent describes that the gateway unit may be separate from, or integrated with, the subscriber terminal:

> A subscriber terminal 60_1, 60_2, … 60_n may be connected to each respective CG 58, or in an alternative embodiment not shown, may be combined with each respective CG 58 to form "converged" CGs 58.

(EX1001, 4:67-5:3).

The specification further explains that the gateway units can be implemented in a *wide* variety of forms, including: a server, a modem, a router, a "module that combines TV, video, internet and voice access," a set top device, "or other fixed or mobile computing, playback, recording, display or communications device," even a phone or VCR. (EX1001, 6:54-62).

Accordingly, a POSA would have understood that the BRI of the term "gateway unit" in the context of the '468 Patent is "a network component that regulates access to a network." (EX1003, ¶¶65-70).

IX. GROUNDS OF UNPATENTABILITY

Pursuant to 37 C.F.R. §42.104(b)(4) and (5), this section demonstrates on an element-by-element basis that claims 1-5, 9, 11-13, 19, 23-27, and 32-34 of the '468 Patent are unpatentable as being obvious in view of *Freund* and *Spusta*. For ease of reference, this analysis includes letters for the individual claim elements (*e.g.*, "1[a]"). This analysis is based on and supported by Dr. Hutchinson's analysis of the '468 Patent and the prior art cited herein. (*See* EX1003).

A. Ground 1: *Freund* Renders Claims 1-5, 9, 12, 19, 23-27, and 33 Obvious

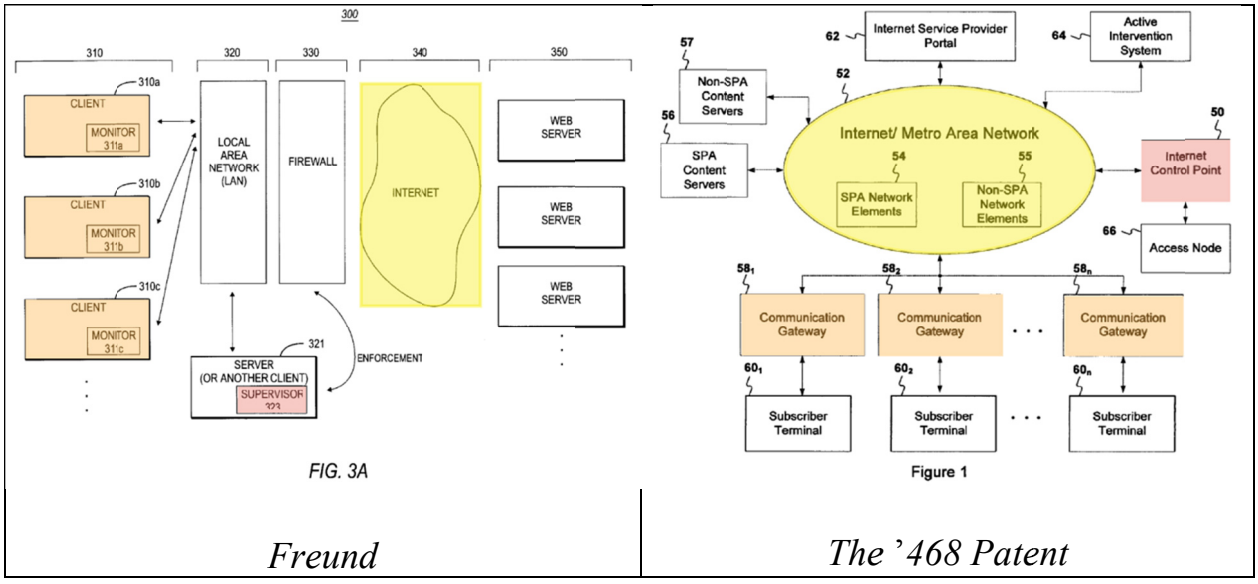
1. *Freund*

Freund describes a "system and methods for client-based monitoring and filtering of access, which operates in conjunction with a centralized enforcement supervisor." (EX1004, 3:51-54). *Freund's* system includes a centralized controller which maintains the access rules for the client based filter, client applications which filter access, and one or more access management applications that set access rules for the entire LAN for one or more workgroups or individual users.

Freund's architecture is virtually indistinguishable from the '468 Patent's architecture. The central controller sends the rules appropriate for a user or workstation to the client-based monitor that allows or denies user access to network servers per the instructions received from the central controller. The instructions can also direct the access monitor to generate notifications when access to particular network servers is attempted or re-direct an access from one network server to another. (EX1004, 28:45-47; 30:52-57; Abstract; EX1003, ¶48).

One embodiment of *Freund's* overall architecture is shown in annotated Fig. 3A (below, left). Highlighted are the client computers with monitors (i.e., the claimed "gateway units") in orange, the supervisor node (i.e., the claimed "controller") in red, and the Internet (i.e., the network to which access is to be

controlled) in yellow. (EX1003, ¶¶49, 73-74, 77). A side-by-side comparison with the architecture of the '468 Patent (below, right) demonstrates the remarkable similarity between the two systems.



Freund | *The '468 Patent*

a. Claim 1[preamble]: "A system for regulating access to a service provider network, the system comprising,"

A "service provider network" is "a network over which services are provided," and the Internet is one such example disclosed in the '468 Patent. (*See supra* Section VIII(A)).

Freund discloses a "system and methods for regulating access and maintaining security of individual computer systems and local area networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet." (EX1004, 1:24-29; EX1003, ¶79).

In addition to providing a system for regulating access to a larger open network, *Freund* also discloses applying its techniques to the open network itself

by explaining that the system "can alternately be implemented for establishing a monitoring and filtering system for Internet Service Providers (ISPs) or similar organizations." (EX1004, 21:50-52; EX1003, ¶80; *see infra* Sections IX(A)(1)(b) and (d)).

b. Claim 1[a]: "a controller node coupled to the service provider network,"

Freund discloses a controller node coupled to the service provider network. In annotated Fig. 3A below, *Freund* describes a "centralized enforcement supervisor" (EX1004, Abstract) on a server or client (13:65-14:5) (hereinafter referred to as a "supervisor node") which, in conjunction with clients, performs monitoring and filtering. A POSA would have understood that the supervisor node is the claimed controller node because it performs the role of determining which users are permitted to contact which network resources. Additionally, in *Freund*, the supervisor node, shown in red below, is connected to a service provider network (the Internet) at a local area network (LAN). (EX1003, ¶83).

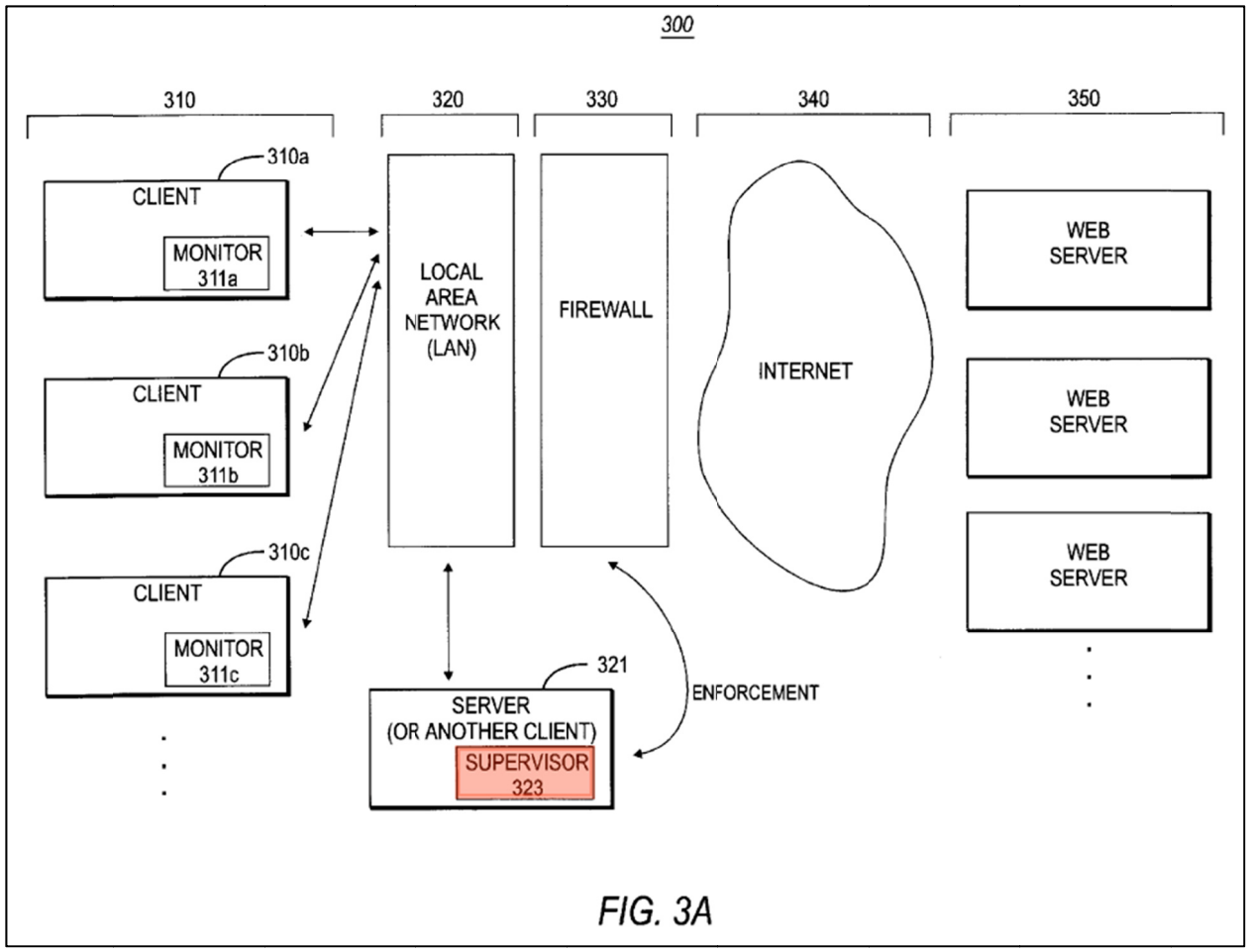


FIG. 3A

Freund explains that the "central supervisor application … maintains the access rules for the client based filter and verifies the existence and proper operation of the client-based filter application." (EX1004, 3:64-67, *see also* 12:54-65). Accordingly, a POSA would have understood that not only does *Freund* disclose a controller node coupled to the service provider network, but that *Freund's* central supervisor application, the supervisor node, performs the same functions as the controller node as claimed. (EX1003, ¶84). *Freund's* service

provider network and the supervisor being coupled to and communicating over this network are described in greater detail with respect to claim 1[c].

c. Claim 1[b]: "the controller node comprising a first processor configured to generate controller instructions, and"

Freund discloses that the supervisor node includes a first processor configured to generate controller instructions because *Freund* discloses that, in some instances, the supervisor node can be implemented using a client with a supervisor component ("The network 320 is connected to a server 321 (or another client) having a supervisor or verifier component") and that clients include processors. (EX1004, 13:65-14:5, 14:52-64, 7:33-43). Annotated Fig. 1 shows this processor:

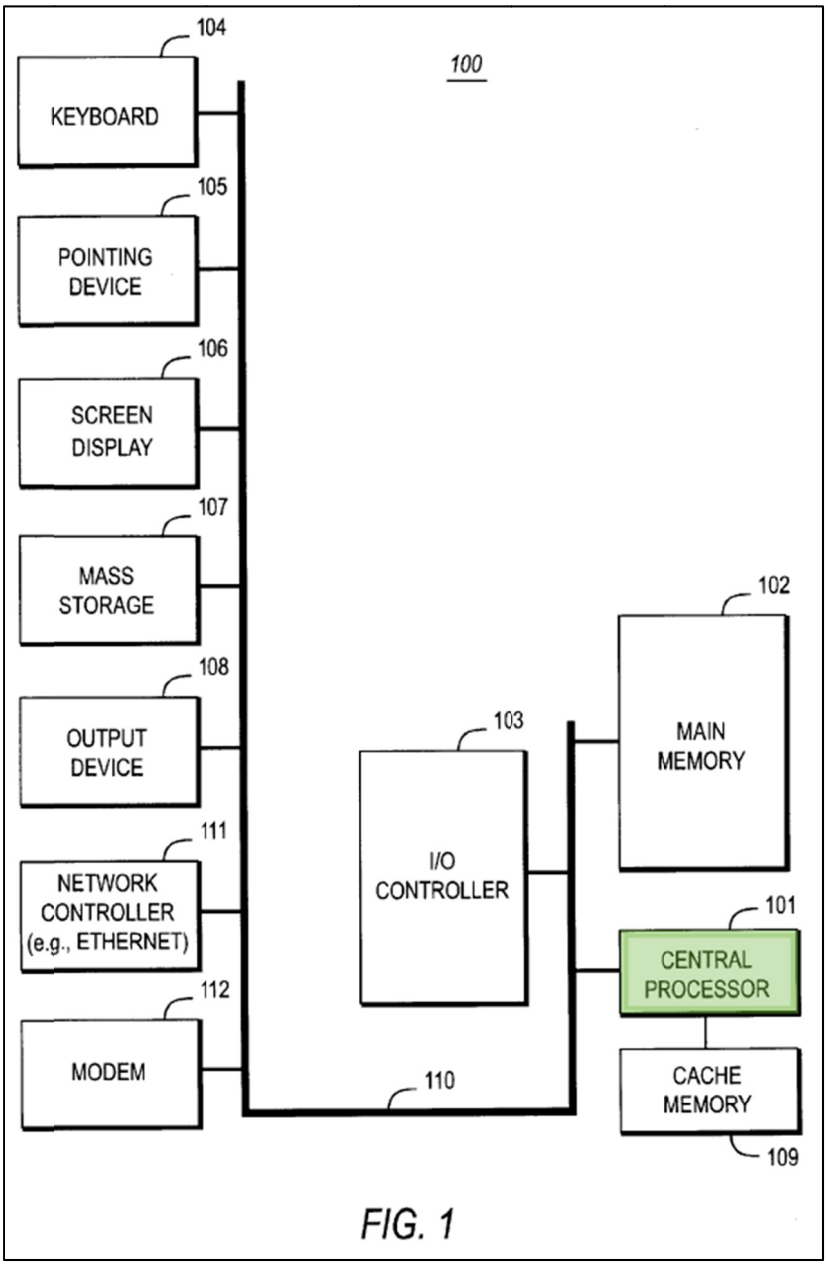


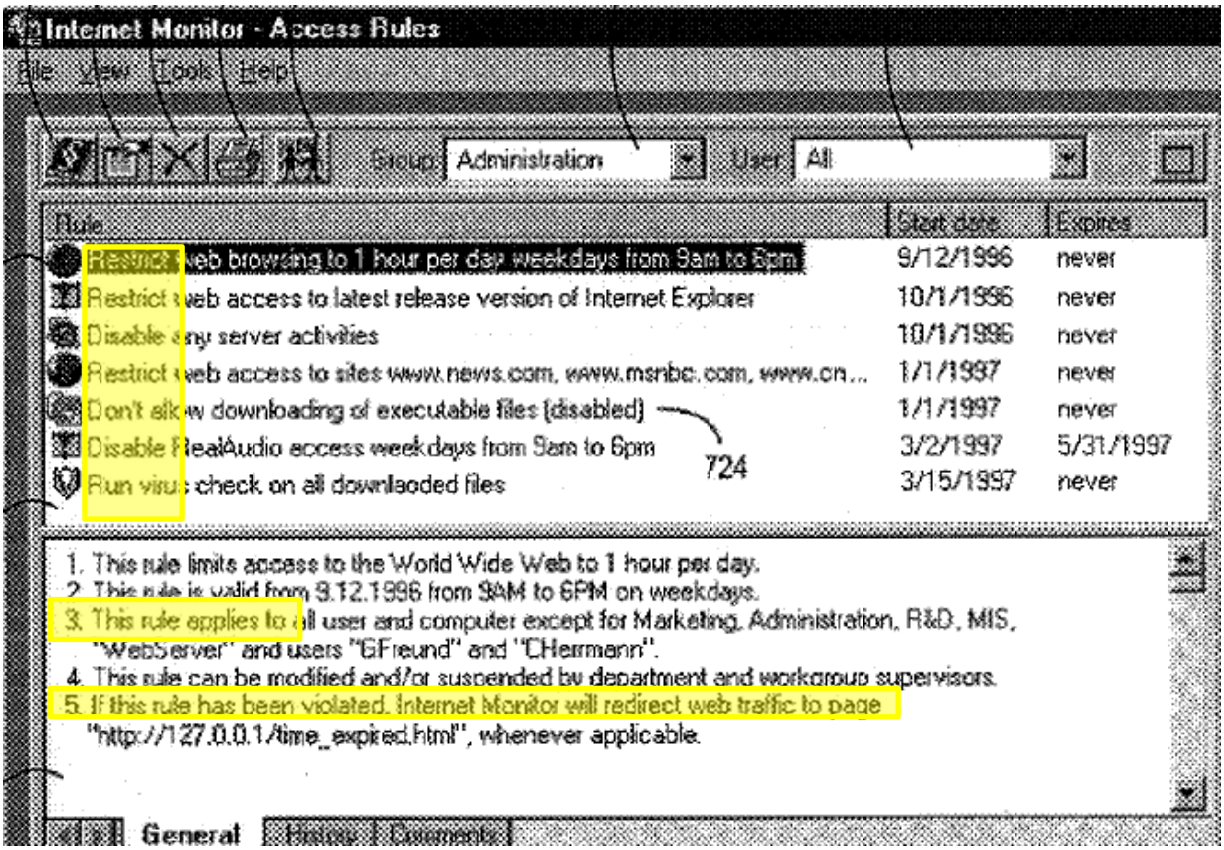
FIG. 1

Moreover, even though *Freund* does not explicitly disclose servers including processors, it would have been obvious to a POSA to include a first processor in the server because, in the case where the network 320 is connected to a server 321, the server would benefit from being comprised of a system such as system 100 like

a client, with well-known computing components such as a processor for carrying out *Freund*'s management functions. (EX1003, ¶86).

Freund discloses that the supervisor node's processor is configured to generate controller instructions as claimed. As discussed, controller instructions are "information sent by the controller that is used to direct the actions of a network unit." In *Freund*, such "instructions" are implemented in the form of "rules" distributed from the controller node/supervisor node: "[t]he system should preferably support centrally-maintained access rules." (EX1004, 8:48-49; EX1003, ¶¶87-89; *see supra* Section VIII(B)).

Examples of *Freund's* rules are shown in the annotated excerpt of Fig. 7A, below. For example, the rules may restrict access to particular websites, may deny access to particular files and services, may be configured to apply to certain users, and may be paired with actions to be performed when those rules are violated, such as redirecting traffic.



Freund explains that the access rules can include "total time a user can be connected to the Internet," "a list of applications … that a user can or cannot use," "***a list of URLs (or WAN addresses) that a user application can (or cannot) access***," etc. (EX1004, 4:8-19 (emphasis added)). A POSA would have understood that *Freund's* "rules" are distributed controller instructions to be enforced by the gateway units because they are sent by the supervisor node (controller) and are information used to direct the actions of a gateway unit, i.e., a network component that regulates access to a network.

Freund's supervisor node also "generates"[2] these rules (the claimed "controller instructions") in multiple ways. For example, *Freund* discloses that rules are "administrator-specified rules" and that the "system allows user (e.g., administrator) configuration of rules which govern use of the protocols monitored by the system." (EX1004, 21:33, 23:66-24:1). Also, it is the "central supervisor application that maintains the access rules." (EX1004, 3:64-65, *see also* Abstract, 5:38-41, 12:54-61). The maintenance of the rules, and in particular the configuration of the rules, constitutes "generating" the rules whenever they are produced or updated. Furthermore, *Freund* discloses that the centralized supervisor application "provides the filter application with the rules [i.e., instructions] for the specific user or workstation" (EX1004, 14:2-5). By "providing" those rules, those rules are therefore produced or "generated" (i.e., from memory or storage). (EX1003, ¶90).

[2] The '468 Patent does not assign any particular meaning to the term "generate" (*see* EX1001, 5:19-22, 6:30-31), but its plain and ordinary meaning is "to produce." (EX1007).

d. Claim 1[c]: "the controller node comprising … a first network interface configured to transmit the controller instructions over the service provider network to a plurality of gateway units; and"

A "gateway unit" is defined as "a network component that regulates access to a network." (*See supra* Section VIII(C)).

Freund discloses a system in which both the supervisor node (i.e., the claimed "controller node"), and clients (i.e., the claimed "gateway units"), are executed on computers configured as shown in annotated Fig. 1 below. (EX1004, 14:52-67; EX1003, ¶96). As shown below, the supervisor node contains a "network controller," shown in purple, which corresponds to the claimed "first network interface."

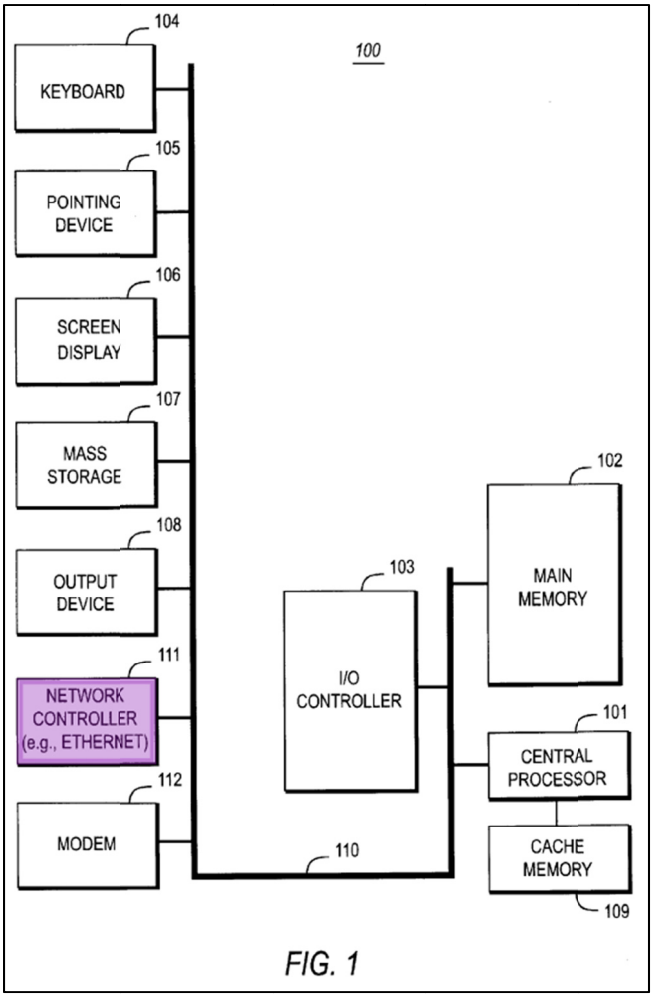


FIG. 1

In at least two embodiments of *Freund*, the network controller is configured to transmit the rules (i.e., the claimed "controller instructions") over the Internet (i.e., the claimed "service provider network") to a plurality of clients (i.e., the claimed "gateway units").

For example, one embodiment is depicted in *Freund's* Fig. 3B, shown below (the embodiment in Fig. 3B is a modification of the embodiment in Fig. 3A discussed further below, *see* EX1004, 21:57-59), In Fig. 3B, central server

component 370 (shown in red) includes the supervisor and is connected to, and communicates with, clients over the Internet. (EX1004, 21:57-22:34).

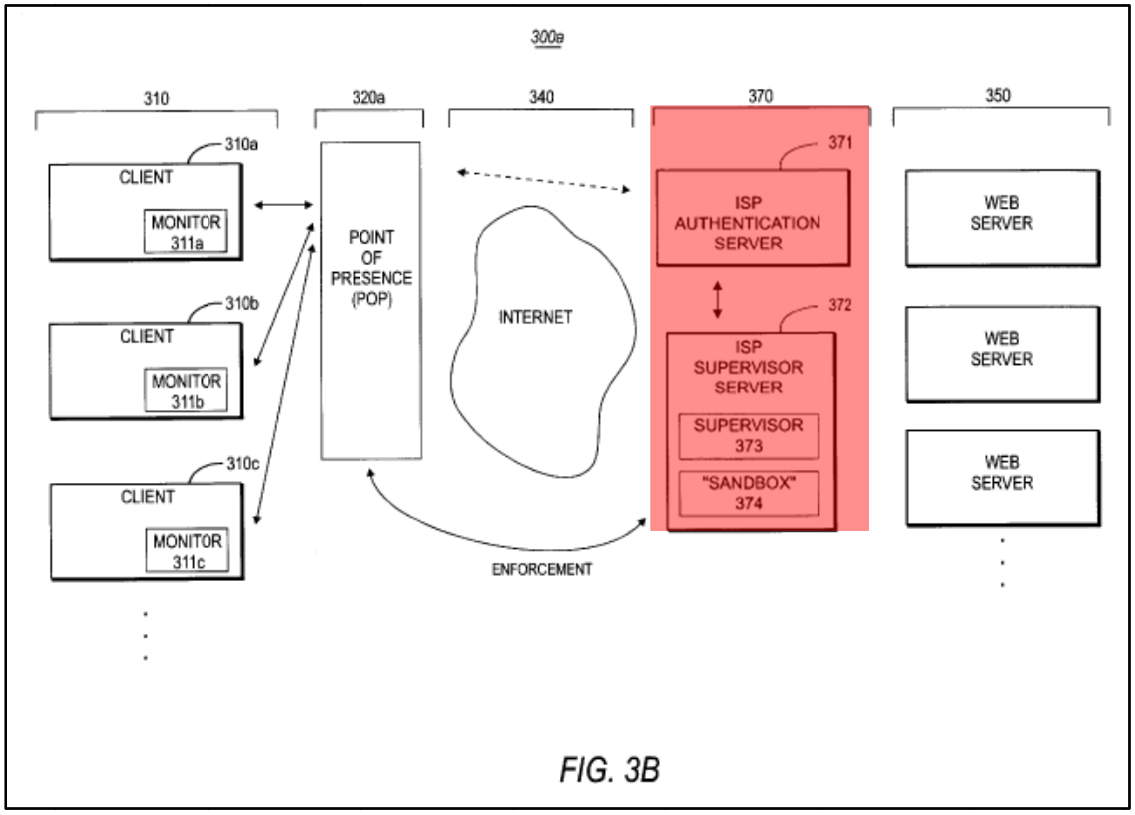


FIG. 3B

With respect to Fig. 3B, *Freund* discloses that the clients (e.g., client 310a) receive access rules (i.e., controller instructions) from the supervisor before users are permitted to use certain network resources. (EX1004, 22:22-31; EX1003, ¶¶98-99).

Another embodiment is depicted in *Freund's* Fig. 3A, shown below, which is an "Internet-based (client/server) system." (EX1004, 14:52-53).

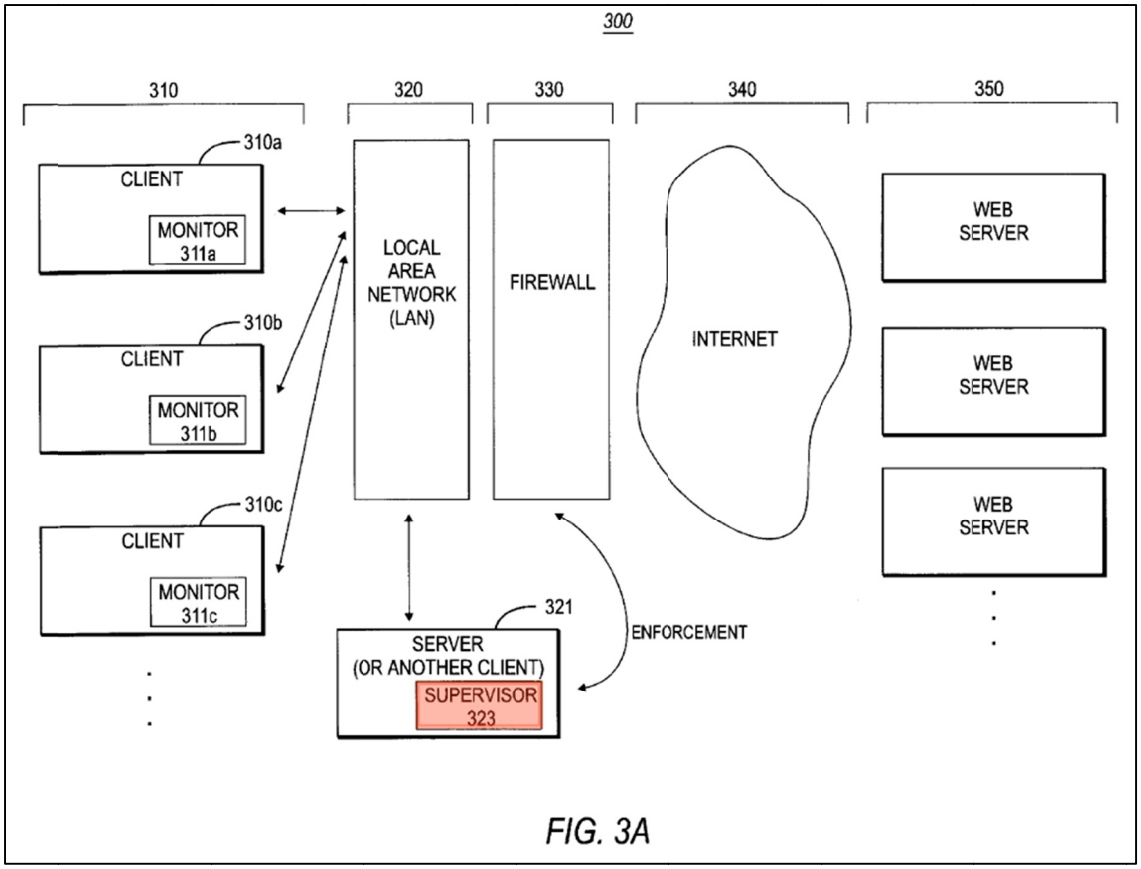


FIG. 3A

With respect to Fig. 3A, the supervisor (shown in red) is also connected to, and communicates with, clients over the Internet. In particular, *Freund* discloses that the clients include client monitors that load and run a filter application. (EX1004, 13:65-14:5; 22:22-27). *Freund* explains that the "centralized supervisor application is installed on a computer on the LAN that can be reached from all workstations" and "monitors whether a client has the filter application loaded and **provides the filter application with the rules for the specific user or workstation**." (EX1004, 13:65-14:5, emphasis added). Thus, *Freund's* supervisor node transmits the rules (i.e., the claimed "controller instructions") to the client

over the server provider network. (EX1003, ¶¶100-101; *See supra* Section VIII(B)).

Also, in the Fig. 3A embodiment, a POSA would have considered LAN 320 to be part of the Internet 340, because, by definition, the Internet is merely the collection of all interconnected networks, which includes LAN 320. (*See supra* Section VIII(A); EX1003, ¶¶102-103; EX1002, p. 53).

But, assuming one were to argue LAN 320 is not part of Internet 340, a POSA would have been motivated to have the computer with the supervisor 323 connected to Internet 340 in situations where the system is used by an organization with widely dispersed geographic locations (perhaps each with its own LAN), and it would have been beneficial and efficient to consolidate all supervisory functions at a single location connected via the Internet. It would therefore have been obvious to transmit rules to be implemented by clients (i.e., the controller instructions) over the Internet, from the supervisor node to the clients, to enable remote management of the clients, and a POSA would have done so with a reasonable expectation of success. (EX1003, ¶103).

e. Claim 1[d]: "the plurality of gateway units,"

A "gateway unit" is "a network component that regulates access to a network." (*See supra* Section VIII(C)).

In annotated Fig. 3A below, *Freund* discloses a plurality of gateway units called clients (shown in orange) and include client monitors, or filter applications (outlined in red). *Freund* explains that the "clients 310*a*, 310*b*, 310*c* … comprise[] a personal computer or workstation, such as system 100" and are "connected to a network." (EX1004, 14:55-57). *Freund* also explains that the client includes "a client-side monitoring component" or filter application, which is the software running on these computers that performs this filtering functionality. (EX1004, 14:59-60).

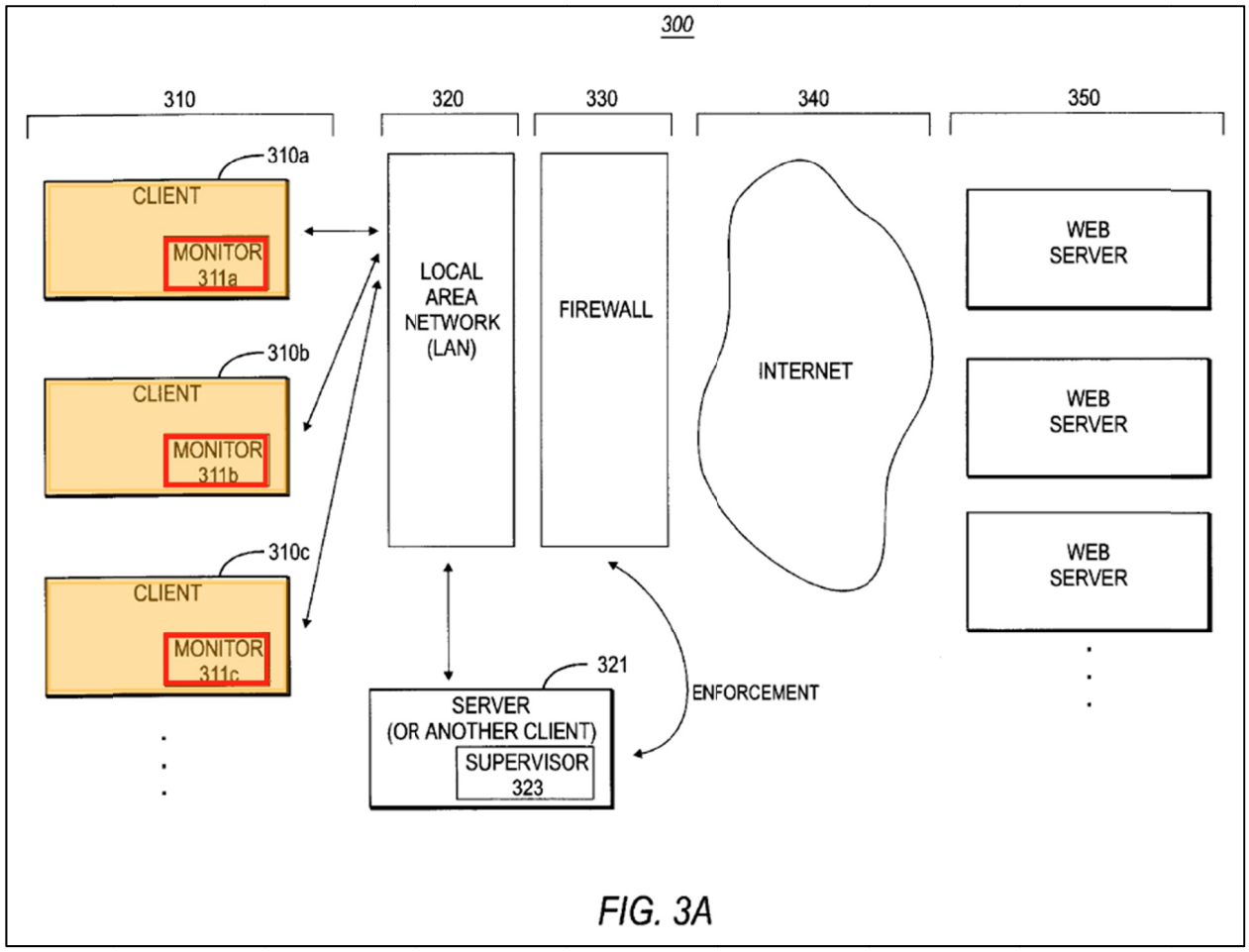


FIG. 3A

Thus, a POSA would have understood that the client machine with the monitor on it constitutes the claimed gateway unit. This configuration in *Freund*, in which the monitor is integrated with the client machine to form a "gateway unit," is one of the options explicitly contemplated by the '468 Patent (*See* EX1001, 4:67-5:3; *supra* Section VIII(C); EX1003, ¶¶106-107).

f. Claim 1[e]: "each of the plurality of gateway units comprising: a user interface configured to receive user-entered content requests for the service provider network,"

Freund discloses a user interface configured to receive user-entered content requests for the network.

Freund discloses software that allows the gateway unit to receive network requests entered by subscribers by describing that standard web browsing clients are executed on the client computer, which receive user-entered content requests for the network. *Freund* explains that "[s]ystem 220 includes a user interface (UI) 260, preferably a Graphical User Interface (GUI), for receiving user commands and data" and that these inputs "may be acted upon by the system 100." (EX1004, 8:11-14). *Freund* also explains that the clients run a "web browser (e.g., Netscape Navigator or Microsoft Internet Explorer…." (EX1004, 15:14-18; EX1003, ¶111).

Annotated Figs. 12A and 12B below show *Freund* teaching user-entered requests that are intercepted by the client monitor, which is on the client (i.e., the claimed "gateway unit").

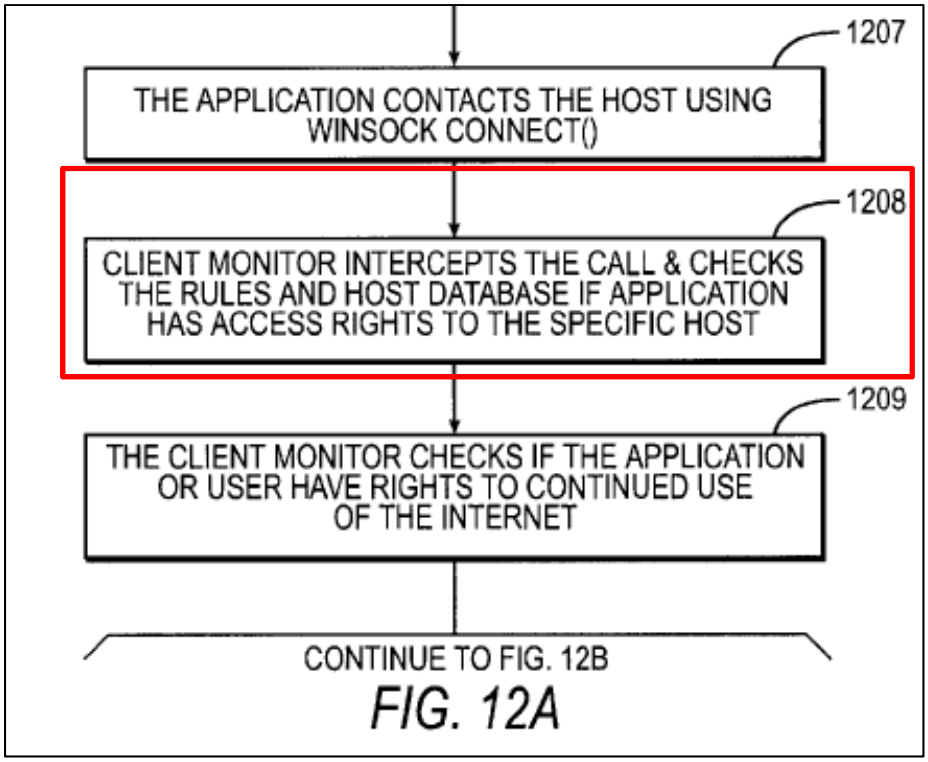
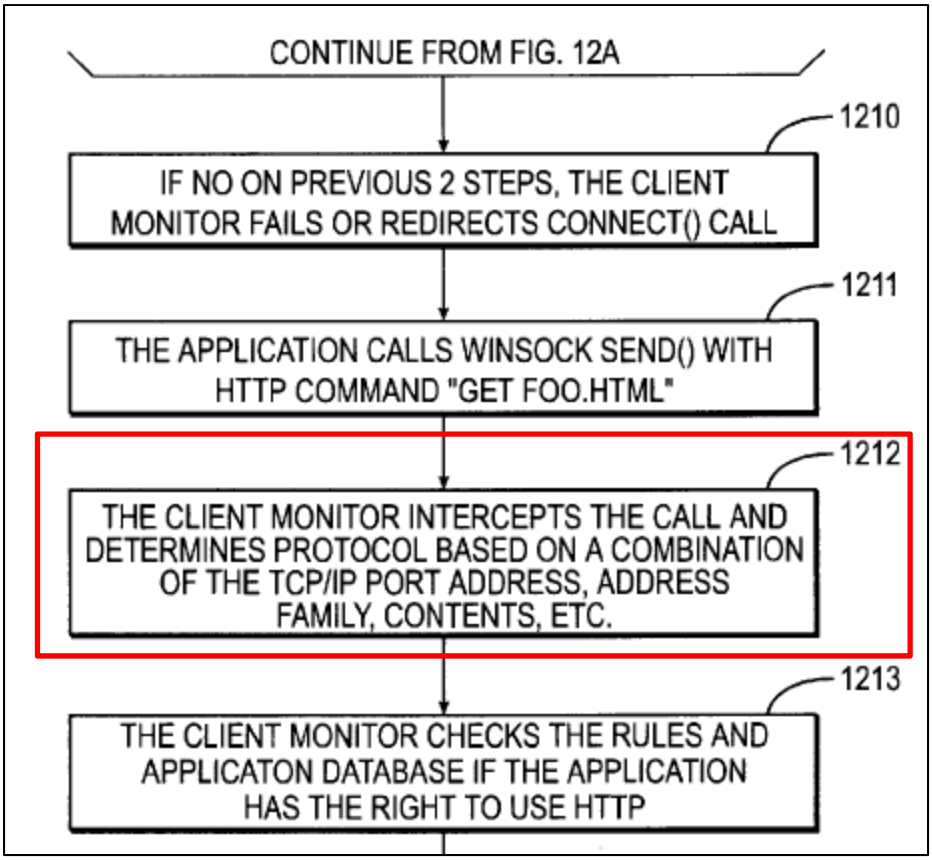

1207
THE APPLICATION CONTACTS THE HOST USING WINSOCK CONNECT()
1208
CLIENT MONITOR INTERCEPTS THE CALL & CHECKS THE RULES AND HOST DATABASE IF APPLICATION HAS ACCESS RIGHTS TO THE SPECIFIC HOST
1209
THE CLIENT MONITOR CHECKS IF THE APPLICATION OR USER HAVE RIGHTS TO CONTINUED USE OF THE INTERNET
CONTINUE TO FIG. 12B

FIG. 12A



Freund also discloses user interface hardware that allows the client to receive network requests entered by subscribers, such as a keyboard, a pointing device, and a screen display, all of which allow the client to receive network requests entered by subscribers via the central processor (i.e., the claimed first processor), shown in annotated Fig. 1 below. (EX1003, ¶112).

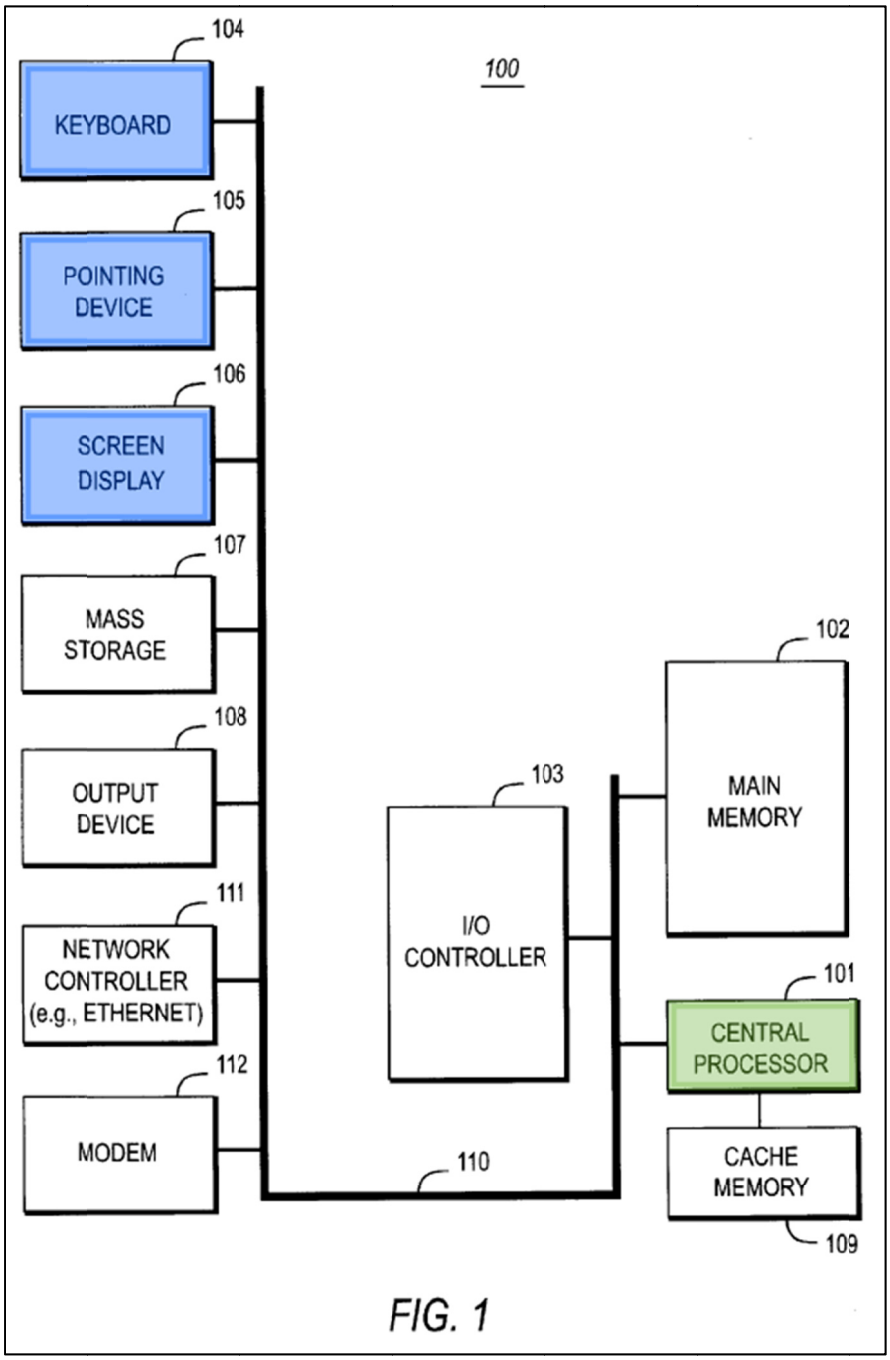

100
104
KEYBOARD
105
POINTING DEVICE
106
SCREEN DISPLAY
107
MASS STORAGE
108
OUTPUT DEVICE
111
NETWORK CONTROLLER (e.g., ETHERNET)
112
MODEM
103
I/O CONTROLLER
102
MAIN MEMORY
101
CENTRAL PROCESSOR
CACHE MEMORY
109
110

FIG. 1

g. Claim 1[f]: "each of the plurality of gateway units comprising … a second network interface coupled to the service provider network and configured to receive the controller instructions from the controller node through the service provider network"

Freund discloses clients (i.e., the claimed "gateway units") being implemented on "a personal computer or workstation, such as system 100" (EX1004, 14:55-57) configured as shown in annotated Fig. 1 below. System 100 contains a network interface 111 shown in gray (the claimed "second network interface").

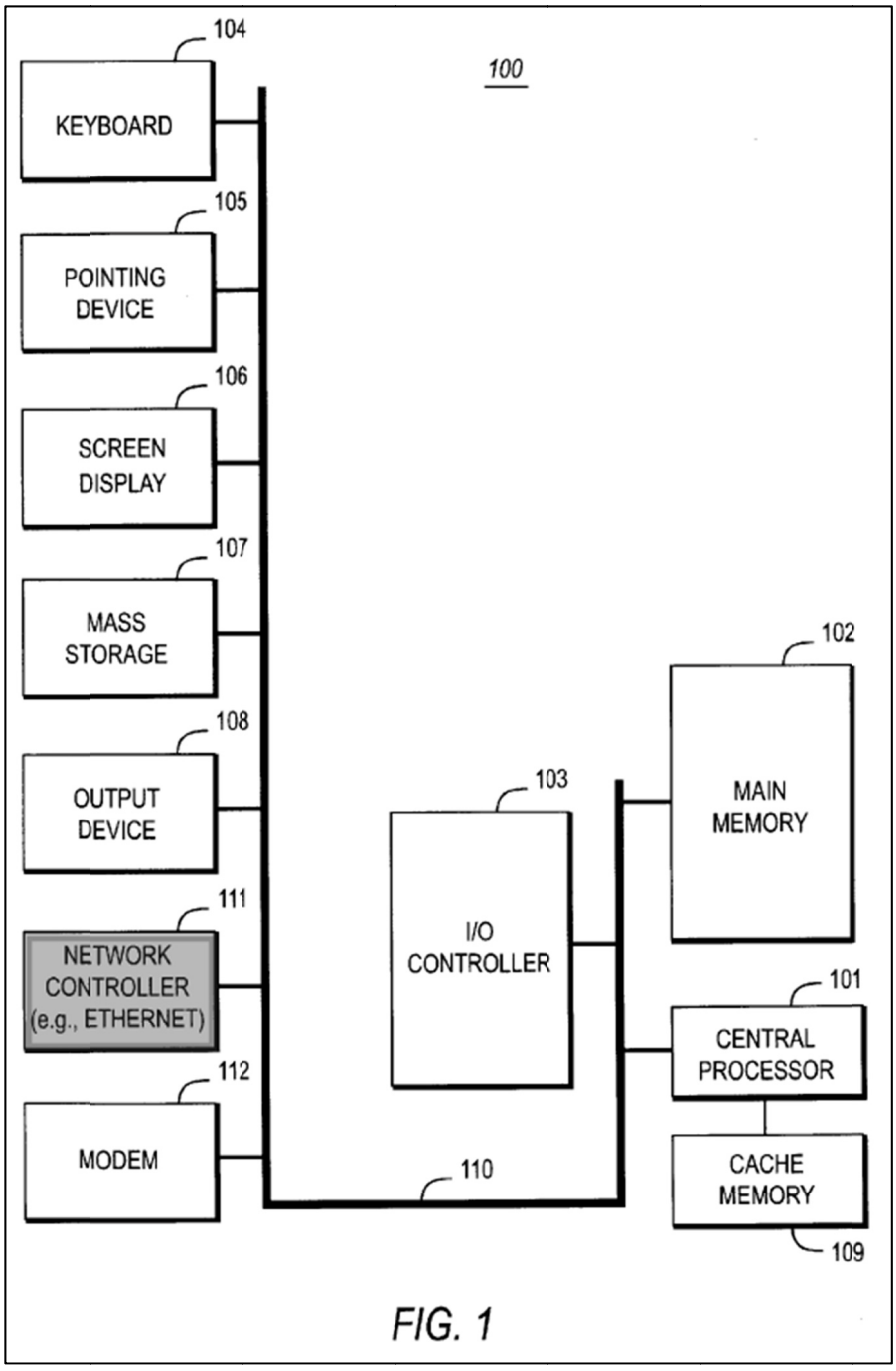


FIG. 1

In the Fig. 3B embodiment, the Network interface 11 is coupled to the Internet via POP 320a, which is "a series of modems to connect client PCs or client LANs, a server or LAN, and one or more router to connect the installation to the Internet." (EX1004, 21:57-64). And over this connection, the network interface will receive

controller instructions. (EX1004, 22:23-27 ("the monitor contacts the central supervisor application 373 on the ISP supervisor server 372 in order to receive access rules")). Additionally, in the Fig. 3A embodiment, network interface 111 is coupled to the LAN, which as described above at claim element 1[c], is part of the claimed "service provider network," and network interface 111 is also configured to receive the controller instructions, or rules, from the controller node through the service provider network. (EX1003, ¶117).

In annotated Fig. 3A below, both the supervisor node (i.e., the claimed "controller node") shown in red, and each client (i.e., the claimed "gateway unit"), shown in orange, have a network interface connected to the network, highlighted in purple and gray, respectively, through which the clients receive the rules (i.e., the claimed "controller instructions") from the supervisor node. Specifically, "[t]he supervisor monitors whether a client has the filter application loaded and provides the filter application with the rules for the specific user or workstation. The filter application maintains a local copy of these rules." (EX1004, 14:2-8; EX1003, ¶118).

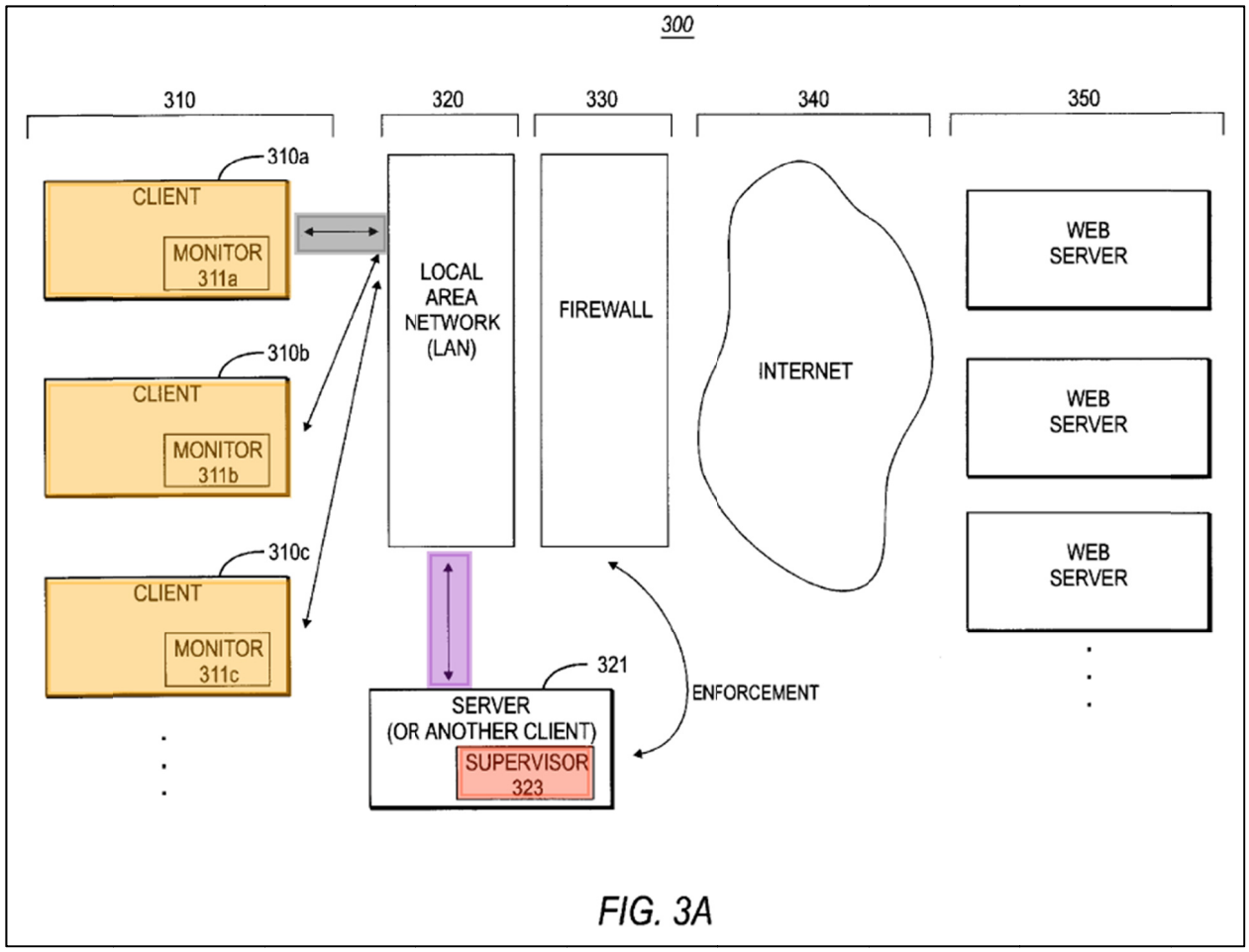


FIG. 3A

h. Claim 1[g]: "each of the plurality of gateway units comprising … a second processor coupled to the user interface and the second network interface"

In the annotated figure below, *Freund* discloses the clients (i.e., the claimed "gateway units") each including a processor, shown in green, coupled to the user interface, shown in blue, and the second network interface, shown in gray. (EX1004, 14:52-67; Fig. 1; EX1003, ¶122).

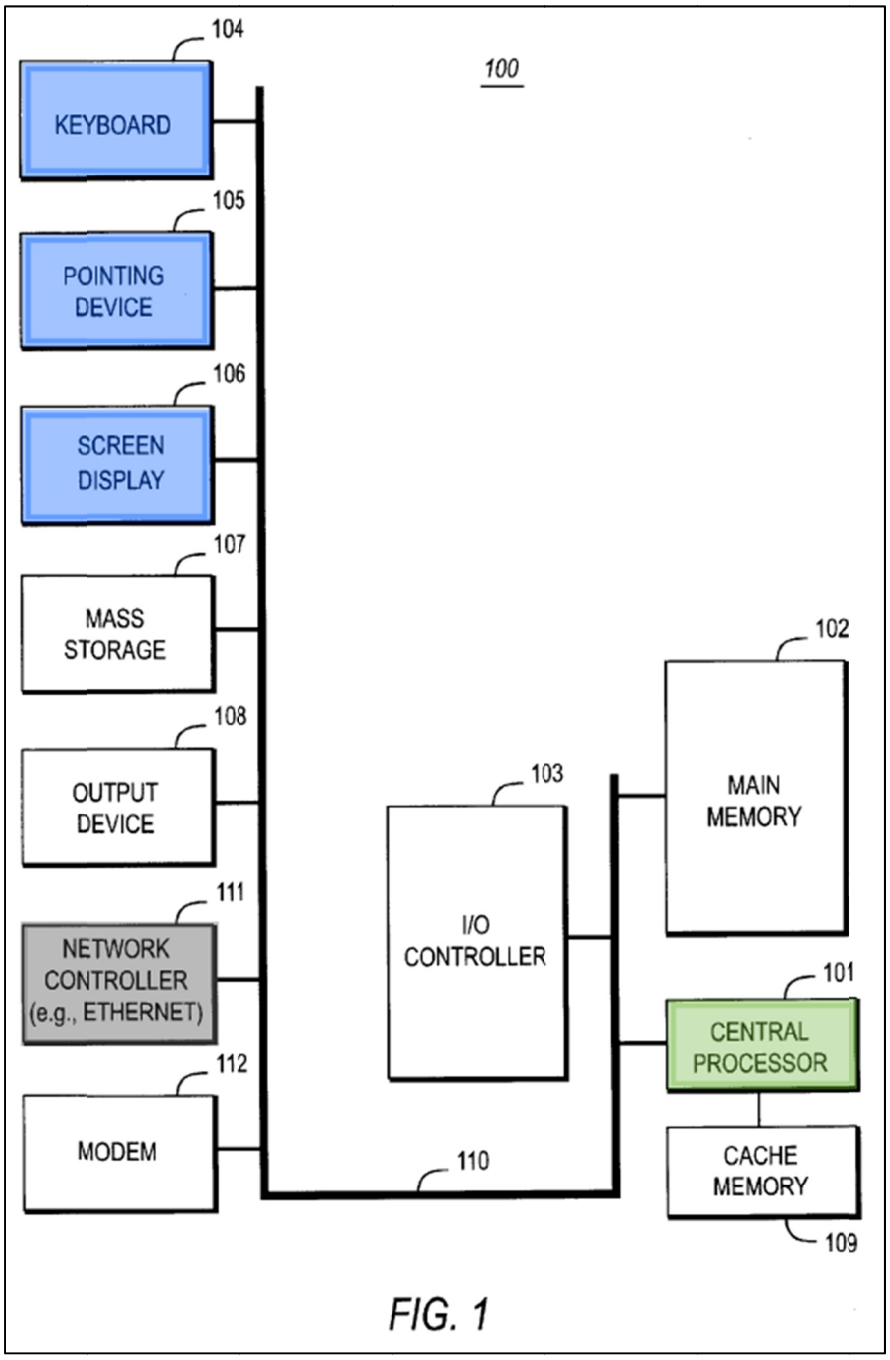


FIG. 1

As explained with respect to claim 1[e], *Freund* discloses both software and hardware that each disclose the claimed user interface. *Freund's* software user interface, e.g., a Web browser (*see* EX1004, 15:16-18), is coupled to the processor because the software is stored in the memory which is coupled to the processor,

and the software instructions are executed by the processor. (EX1004, Fig. 1; EX1003, ¶123). *Freund's* hardware user interface components (e.g., the keyboard, the pointing device, and the screen display) are coupled with the second processor by the bus 110. (*See also supra* Section IX(A)(1)(f); EX1003, ¶124).

i. Claim 1[h]: "wherein the second processor is configured to selectively transmit the content requests to the service provider network in accordance with the controller instructions, and transfer received content data responsive to the transmitted content requests from the service provider network via the second network interface."

Freund discloses software, boxed in red below, running on the client, shown below in orange, that selectively allows and blocks a user's Internet access requests based on rules received from the supervisor node as claimed. In annotated Fig. 3A below, *Freund* discloses "a client-side monitoring component for monitoring Internet access in accordance with the present invention, as specifically shown at 311a, 311b, and 311c." (EX1004, 14:59-62). This software runs on the client's processor. (EX1004, 14:52-62; EX1003, ¶129).

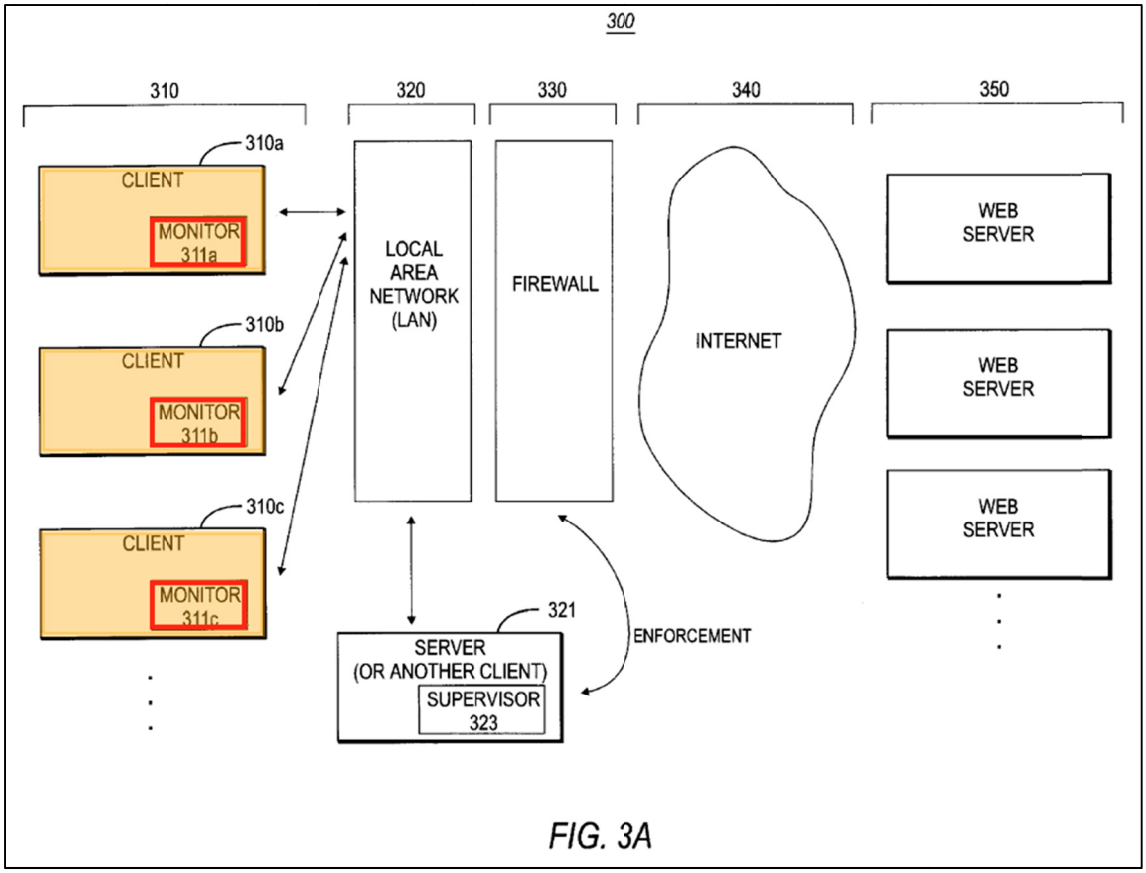


FIG. 3A

Freund discloses that the client monitor, via its data acquisition module, is configured to selectively transmit the content requests to the service provider network in accordance with the controller instructions. (EX1004, 15:26-16:3). *Freund* further explains that:

> By intercepting and interpreting all TCP/IP communication and building a comprehensive representation of these TCP/IP activities, the system can monitor TCP/IP activities on a per process or per application basis. If a particular process has access rights to the Internet (and is permitted to use the detected protocol and no other rules are violated), the communication of the process is logged and allowed to go forward. Otherwise, the prescribed remedial action for

> any violated rule is performed, including logging an exception log entry and, depending on the rules the TCP/IP activity, the communication is either terminated, redirected, modified, or continued.

(EX1004, 4:50-62; EX1003, ¶130).

Freund also discloses that if Internet access is allowed, then the requested content is transmitted from the Internet (i.e., the claimed "service provider network") via the network controller (i.e., the claimed "second network interface"). As discussed above, and shown in annotated Fig. 3A below, *Freund* discloses "a client-side monitoring component for monitoring Internet access in accordance with the present invention, as specifically shown at 311a, 311b, and 311c." (EX1004, 14:59-62). This software, boxed in red, runs on the client's processor (EX1004, 14:52-62; EX1003, ¶131).

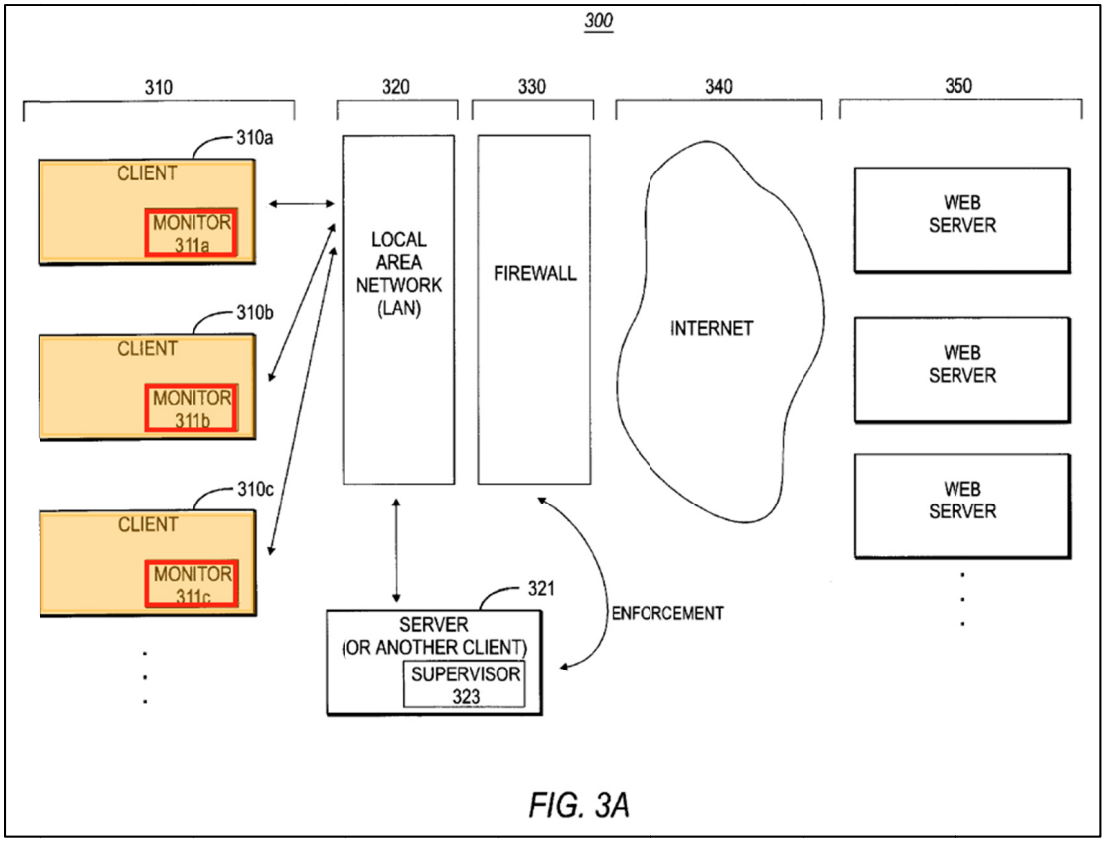


FIG. 3A

Additionally, *Freund* explains that if an application has access to the Internet, various commands can be issued for retrieving information from a Web site, and "[i]n response to these requests, the corresponding server at the Web site sends appropriate responses, including transmitting requested content." (EX1004, 19:51-57)." And, as shown in Fig. 3A, the requested content is transmitted via the Internet (including LAN) service provider network to the client (i.e., the claimed "gateway unit"), which includes the second processor and second network interface. (*See also supra* Sections IX(A)(1)(c)-(d) and (g), including a discussion of *Freund's* Fig. 3B; EX1004, 22:23-27; EX1003, ¶132).

j. Claim 2[preamble]: "The system of claim 1 wherein,"

See supra Sections IX(A)(1)(a)-(i).

k. Claim 2[a]: "each of the gateway units further comprises a storage device configured to store the controller instructions; and"

Freund discloses that each client (i.e., the claimed "gateway units") further comprises a storage device 107, shown in light blue in annotated Fig. 1 below, configured to store the rules (i.e., the claimed "controller instructions"). *Freund* explains that "[t]he filter application maintains a local copy of these rules so that rule enforcement continues even when the user accesses the Internet but bypasses the LAN (e.g., a mobile computer on the road)." (EX1004, 5:12-15, *see also* 13:65-14:8; 21:33-40; EX1003, ¶136).

Additionally, "[a]ccess rules are still enforced because Client Monitor employs a local copy of rules (previously downloaded)." (EX1004, 6:26-27; EX1003, ¶136).

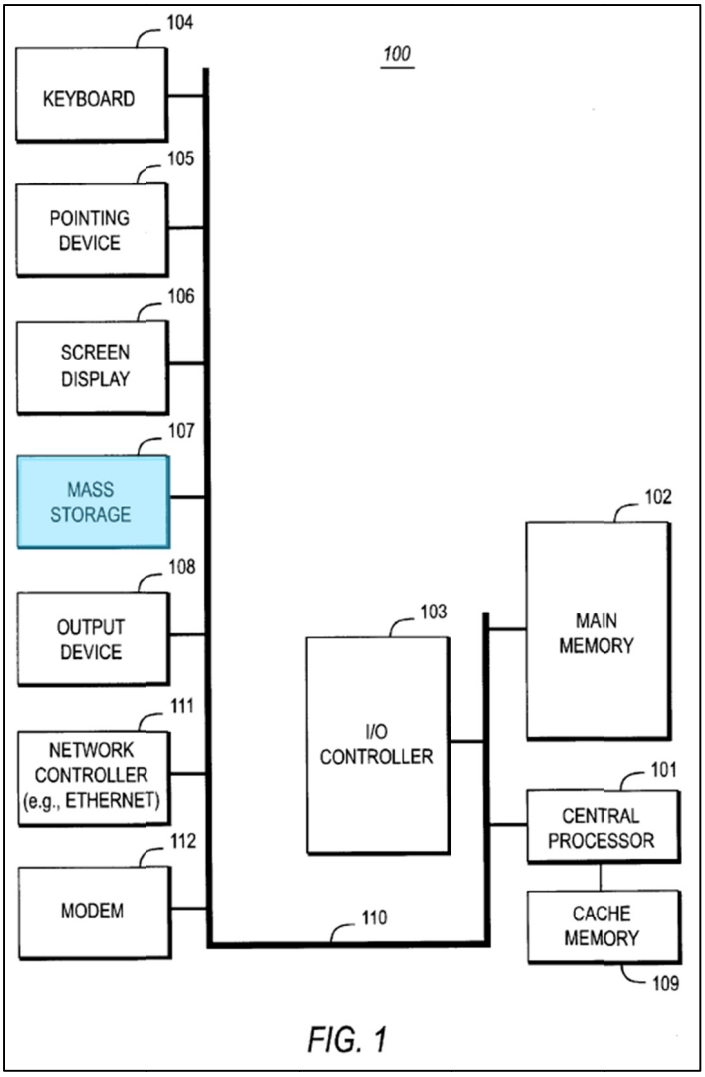


FIG. 1

l. Claim 2[b]: "each the gateway units has an identifier that uniquely identifies the gateway unit."

When discussing the process of creating rules (i.e., the claimed "controller instructions"), *Freund* indicates that computers, the physical machines that contain the client monitor software, have unique IP addresses which serve as unique identifiers. "A 'computer,' on the other hand, represents an individual workstation or other device connected to the system; typically, such a device has a unique IP address assigned to it." (EX1004, 26:32-35). *Freund* also discloses an

initialization of the system that includes the management of specific clients (i.e., the claimed "gateway units"), including "send[ing] a login request to the Supervisor," "the Supervisor check[ing] if the Client Monitor (computer/user) has any Internet access rights," and "the Supervisor determin[ing] the department or workgroup for the Client Monitor." (EX1004, 28:3-13). It would have been necessary, or at least obvious, to a POSA, to perform these functions using unique identifiers for each client, thereby permitting the supervisor to custom-manage each of the clients individually, since *Freund*'s rules are not only global rules applied uniformly across a network. (EX1004, 4:19-21 ("to whom should a rule apply (list of users, list of workgroups, or all")).. (EX1003, ¶138).

Additionally, *Freund* discloses in annotated Fig. 7F below that rules can apply to specific computers, which include the client monitor software. Each local computer (gateway unit) is identified in the rules via a unique identifier. The computer which is being added to the rule is called "WebServer." (EX1003, ¶139). Thus, *Freund* discloses, or at least renders obvious, this limitation by showing that rules, which are applicable to specific chosen computers, would have identified those computers by a unique name.

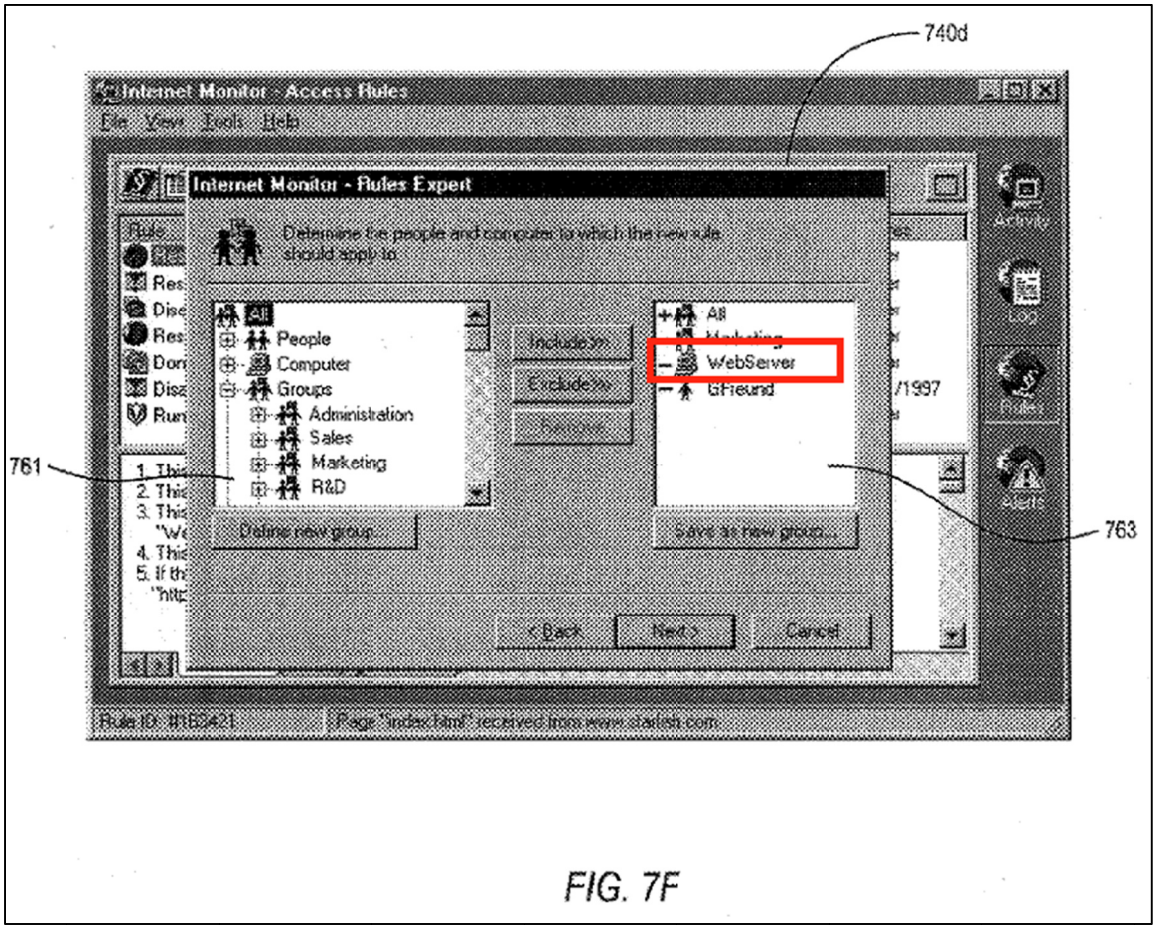


FIG. 7F

m. Claim 3[preamble]: "The system of claim 1"

See supra Sections IX(A)(1)(a)-(i).

n. Claim 3[a]: "wherein the controller instructions include instructions configured to deny access to a first group of network servers of the service provider network."

In annotated Fig. 7A below, a POSA would have understood that *Freund* discloses that the rules (i.e., the claimed "controller instructions") include specific rules configured to deny access to a first group of network servers of the Internet (i.e., the claimed "service provider network").

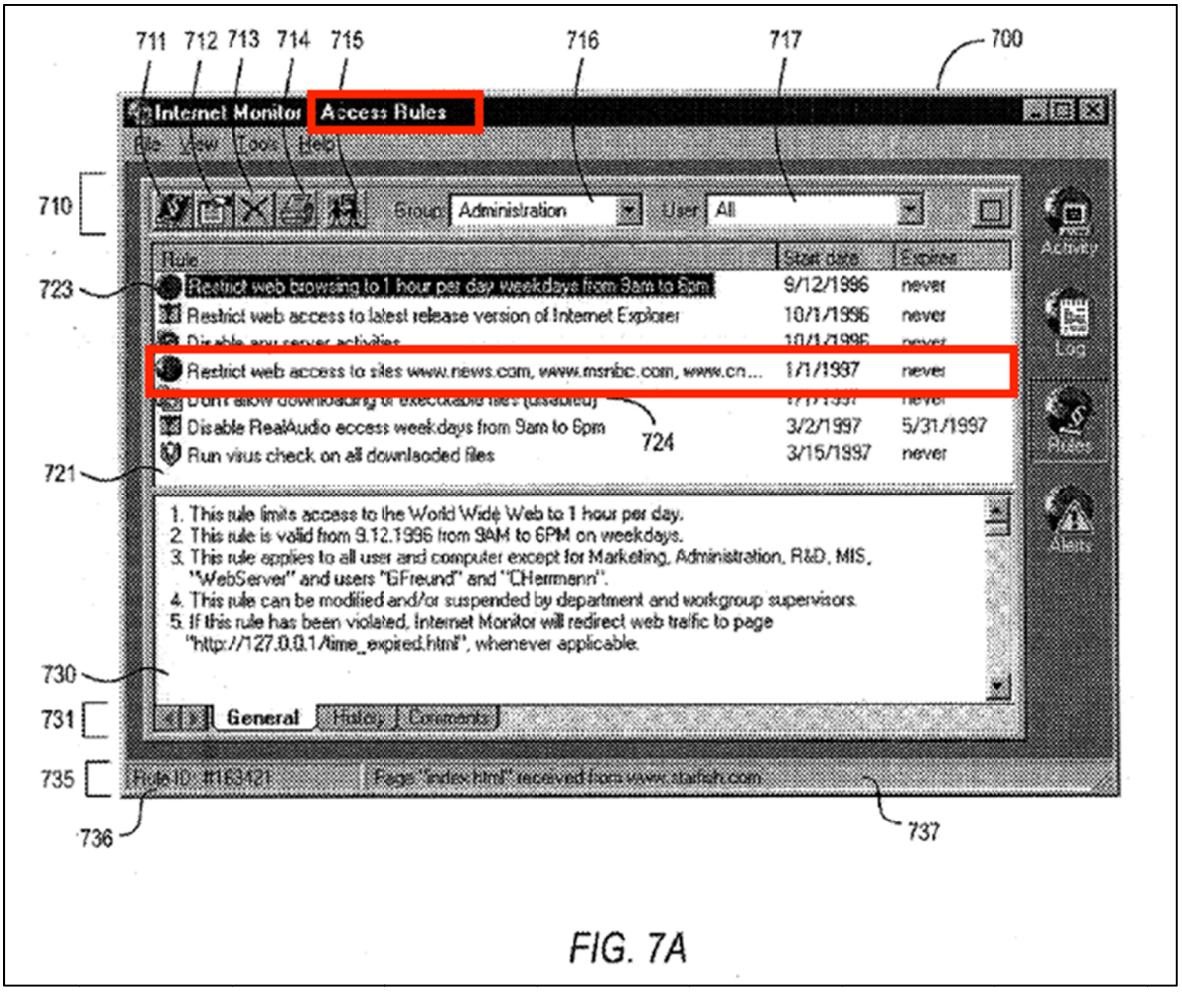


FIG. 7A

The highlighted fourth rule says, "Restrict web access to sites www.news.com, www.msnbc.com, www.cn…." This controller instruction is configured to "restrict" access to the listed group of network servers and thus "deny" access to all other network servers.

Freund further discloses that "access rules can include criteria such as … a list of URLs (or WAN addresses) that a user application can (or cannot) access" (EX1004, 4:8-19) and "what should happen if a rule is violated (e.g., denying

Internet access, issue a warning, redirecting the access, creating a log entry, or the like)." (EX1004, 4:19-29, 13:13-23; EX1003, ¶142).

o. Claim 4[preamble]: "The system of claim 3,"

See supra Sections IX(A)(1)(m)-(n).

p. Claim 4[a]: "wherein the controller instructions comprise instructions configured to generate a notification to the controller node if a content request designates a network server of the service provider network."

Freund renders obvious that the rules (i.e., the claimed "controller instructions") can be configured to generate a notification to the supervisor node (i.e., the claimed "controller node") when a content request designates a network server of the Internet (i.e., the claimed "service provider network").

Freund discloses that the rules include instructions governing "what should happen if a rule is violated (e.g., denying Internet access, issue a warning, redirecting the access, creating a log entry, or the like)." (EX1004, 4:19-29, 13:13-23). As discussed with respect to claim 3 above, an example of a rule in *Freund* is to deny access to network servers of the service provider network, and therefore violations of this rule include content requests to those denied network servers. A POSA would have understood that the warning or log entry for such a violation could be generated anywhere in the network, and a POSA would have been motivated to generate either notification to the supervisor node, or controller node, so that a system administrator would know of the rule violation and be alerted to

take action if necessary. This would have been an obvious matter with predictable results because it would have been desirable to alert the administrator so that action could be taken if the violations continued and no unforeseen results would occur from doing so. (EX1003, ¶147).

q. Claim 5[preamble]: "The system of claim 3, wherein the controller instructions are further configured to:"

See supra Sections IX(A)(1)(m)-(n).

r. Claim 5[a]: "detect a content request that designates a first network server of the service provider network; and"

In annotated Fig. 7A below, *Freund* discloses that the rules (i.e., the claimed "controller instructions") can be configured to detect a content request that designates a first network server of the Internet (i.e., the claimed "service provider network"). (EX1003, ¶149).

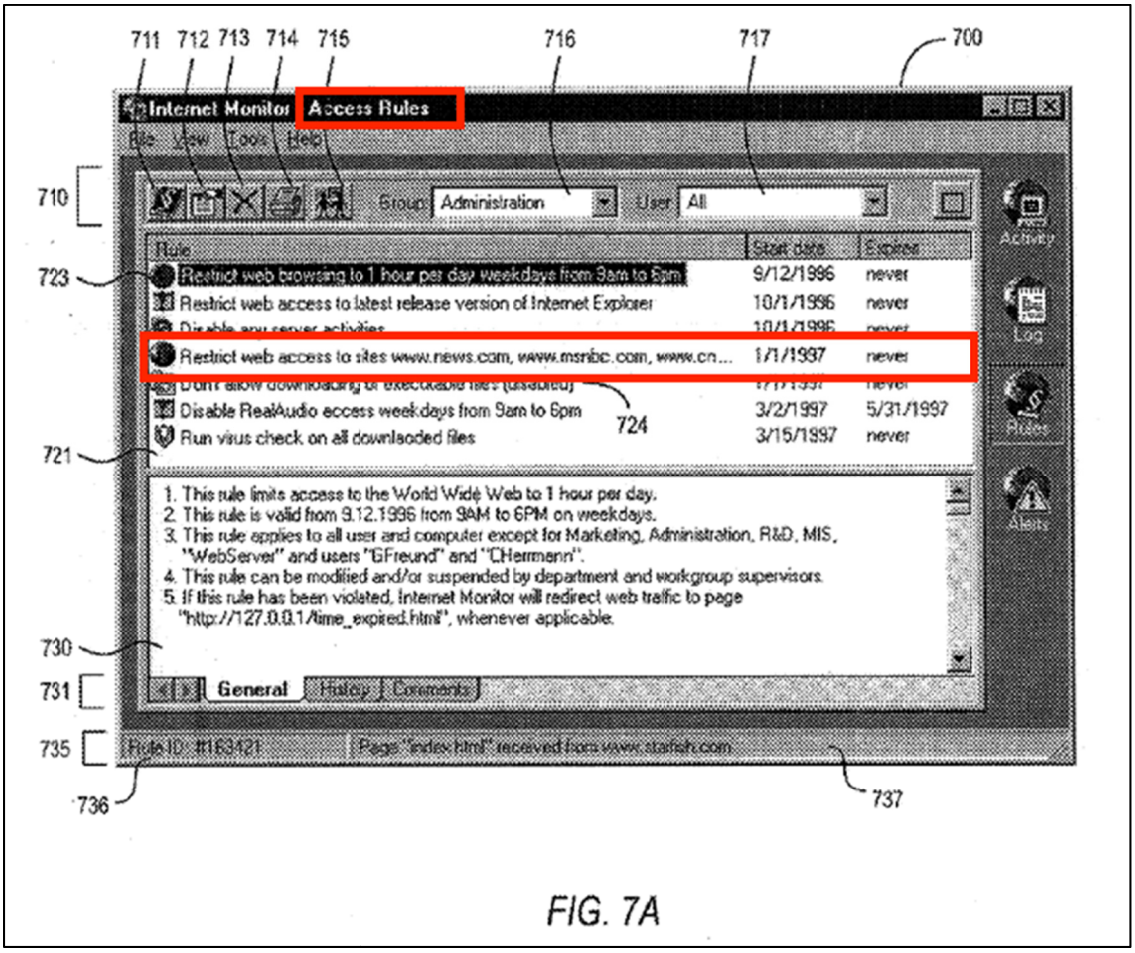


FIG. 7A

The highlighted fourth rule says, "Restrict web access to sites www.news.com, www.msnbc.com, www.cn…." This rule is configured to detect a content request designating a first network server such as any network server not in the listed group of restricted-access network servers. (EX1003, ¶150).

s. Claim 5[b]: "re-direct the content request to a second network server of the service provider network."

Freund further discloses that a rule can be configured to re-direct the content request to a second network server (i.e., another website) of the Internet (i.e., the claimed "service provider network").

Freund discloses that a rule includes "what should happen if a rule is violated (e.g., denying Internet access, issue a warning, redirecting the access, creating a log entry, or the like)." (EX1004, 4:19-29, 13:13-23). "For instance, a request to access a particular Web site can be patched to instead redirect that request to another site." (EX1004, 21:15-17, *see also* 21:21-40; EX1003, ¶151).

t. Claim 9: "The system of claim 1, wherein the controller instructions are configured to place a gateway unit in a user-controlled operational mode on receipt of permission from the controller node."

The '468 Patent does not define what a "user-controlled operational mode" is and does not use this phrase, nor the phrase "user-controlled" nor "operational" nor "mode" except when talking about the deadman switch or advertising, which is inapplicable here. (EX1001, 4:6-48). Despite this, a POSA would have understood that the user-controlled operational mode is a mode where the user is controlling the gateway unit's operation based on the plain meaning of the phrase's constituent words. (EX1003, ¶152).

A POSA would have recognized that *Freund's* system would include rules (i.e., the claimed "controller instructions") configured to place a client (i.e., the claimed "gateway unit") in a user-controlled operational mode on receipt of permission from the supervisor node (i.e., the claimed "controller node") to allow the user to customize the rules that control how the user is allowed to access the network.

Freund discloses, "[t]he system should preferably support centrally-maintained access rules (e.g., defining basic access rights), but at the same time allow individual workgroup managers or even individual users to set rules for their area of responsibility, if so desired by the organization." (EX1004, 8:48-53). Therefore, a POSA would have been motivated to have the supervisor node put the client into a user-controlled operational mode to allow the local user or workgroup manager to set rules. *Freund's* user-controlled operational mode would be when the workgroup or department supervisor or the local user (as opposed to the system-wide administrator user) is using the rule editor to view or modify rules. (EX1004, 13:13-23, 27:19-36, *see also* 4:19-29; EX1003, ¶¶153-154).

A POSA would thus have recognized that *Freund* discloses that the supervisor, by sending rules that may be viewed and modified by the local workgroup or department supervisors or the end user himself, provides permission so that the system can be put into a user-controlled operational mode where the

user can use the rule editor to view or modify rules. (EX1003, ¶155; *see supra* Sections IX(A)(1)(a)-(i)).

u. Claim 12[preamble]: "The system of claim 1, wherein the controller instructions are configured to enable a gateway unit to:"

See supra Sections IX(A)(1)(a)-(i)).

v. Claim 12[a]: "receive registration information via the user interface;"

Freund discloses that the system can receive registration information via the user interface. In describing how the client monitor on the client (i.e., the claimed "gateway unit") is loaded, *Freund* discloses "the Client Monitor sends a login request to the Supervisor, at step 802." (EX1004, 28:7-8). Before the client monitor can send this login request to the Supervisor, it must have received the necessary login (registration) information from the user via the user interface. In an alternative embodiment, *Freund* describes this same step in more detail "[a]t step 1101, the RAS calls the ISP POP server using SLIP, PPP or similar protocol with user ID/password." (EX1004, 28:57-59). A POSA would have understood this to mean the user entered their user ID and password into a client application, software user interface, or via a keyboard or pointing device, hardware user interface. (*See supra* Section IX(A)(1)(f); EX1003, ¶158).

w. Claim 12[b]: "transmit the registration information to the controller node; and

Freund discloses transmitting the registration information to the supervisor node (i.e., the claimed "controller node"): "[a]t step 1105, the Client Monitors send login requests to the ISP Supervisor." (EX1004, 29:1-3; EX1003, ¶159).

x. Claim 12[c]: "on registration, receive initial operating parameters from the controller node via the second network interface."

The '468 Patent describes "initial operating parameters" as "includ[ing], for example, the address of the CG's 58, ICP 50 and other variables." (EX1001, 7:29-31). While the "other variables" are not described, a POSA would have understood that "initial operating parameters" would have been configuration information that allows the gateway units to perform its functions. (EX1003, ¶160).

Freund discloses that, upon registration, both rules and additional information are received by the clients from the supervisor node: "[t]he Supervisor then transmits access rules *and the like* to the Client Monitor at step 1106." (EX1004, 29:3-4, emphasis added, *see also* Fig. 2). It would have been obvious to a POSA to include additional information such as configuration information (initial operating parameters) because it is the supervisor node's responsibility to "dynamically set the addresses of the workstations that should have access to the

Internet," "monitor whether a client has the filter application loaded," and to "coordinate[] the system." (EX1004, 5:21-24; 14:2-5; 14:33-34; EX1003, ¶161).

A POSA would have understood that many network components, including clients, require "operating parameters" or configuration information to operate correctly. For example, a client would need to know how to communicate with its assigned supervisor node. A network component can only obtain this information in one of two ways: (1) either the information is loaded into the device statically when it is created; or (2) the information is received dynamically sometime later. Thus, a POSA would have seen that it is a simple design choice whether to load these operating parameters into the device statically, or to receive them dynamically. (EX1003, ¶162).

A POSA would have also understood that receiving these operating parameters dynamically would provide the advantage of increased flexibility; the device would adapt to changes in the operating environment more easily by receiving these operating parameters dynamically rather than statically. The obvious candidate from which to receive these initial operating parameters is from the supervisor node (controller node) at registration time to facilitate the correct operation of the filtering application. This is obvious because the supervisor node is responsible for "dynamically set[ting] the addresses of the workstations that should have access to the Internet," "monitor[ing] whether a client has the filter

application loaded [(installed)]," and "coordinat[ing] the system." (EX1004, 5:21-24; 14:2-5; 14:33-34; EX1003, ¶¶162-163; *see also supra* Section IX(A)(1)(g)).

y. Claim 19[preamble]: "The system of claim 1, further comprising"

See supra Sections IX(A)(1)(a)-(i)).

z. Claim 19[a]: "a plurality of access nodes coupled to the service provider network,"

In annotated Fig. 3B below (a modification of the Fig. 3A embodiment, EX1004, 21:57-59), *Freund* discloses a Point of Presence (POP) (the claimed "access nodes") coupled to the service provider network. (EX1003, ¶¶172-173; *see also* EX1004, 21:59-64).

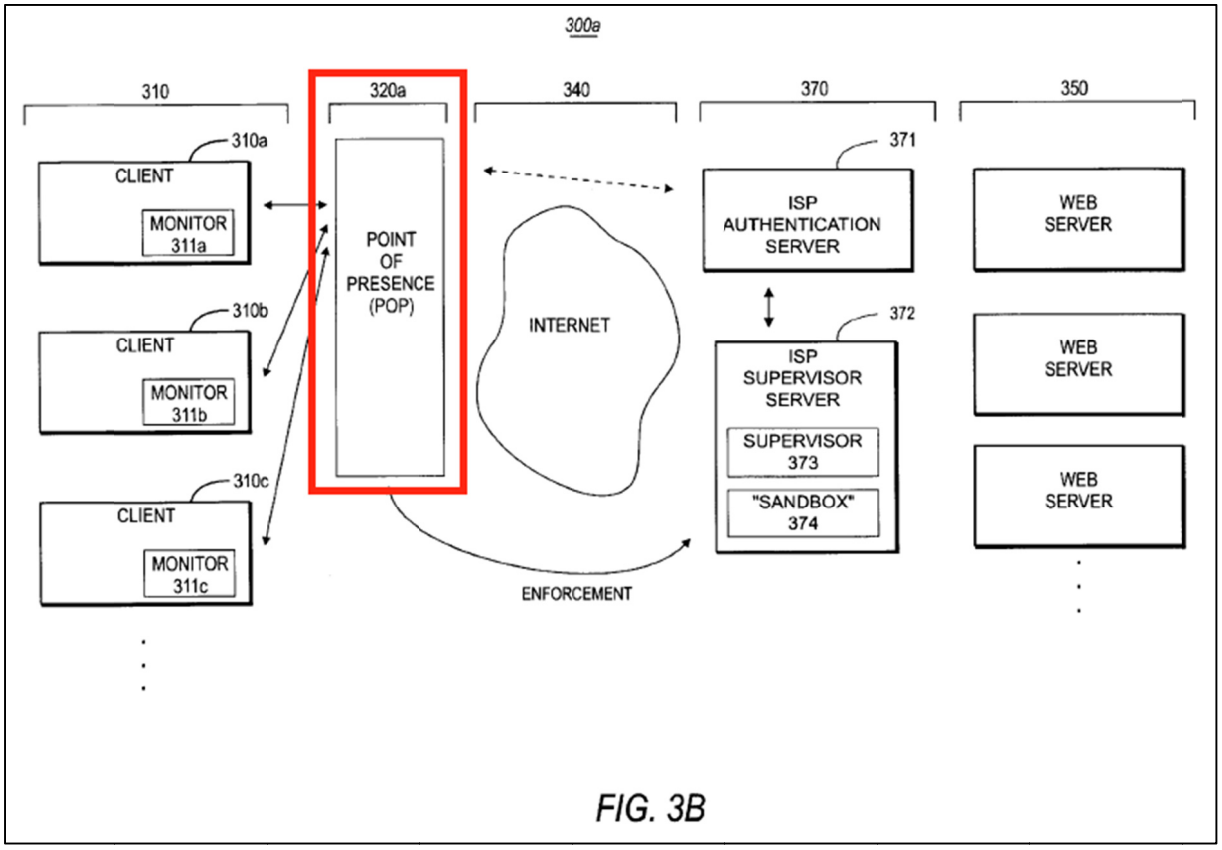


FIG. 3B

Although this figure shows only one POP, *Freund* explains "ISPs normally have one or more POPs in the areas that they serve." (EX1004, 21:64-65; EX1003, ¶173; *see also infra* Section IX(A)(1)(aa)).

aa. Claim 19[b]: "wherein the controller node is further configured to generate authorization instructions and transmit the authorization instructions over the service provider network to the access nodes, and"

Freund discloses, in the embodiment depicted by Fig. 3B, that its controller node is configured to generate and transmit authorization instructions, as claimed by the '468 Patent. In Fig. 3B., the central server component 370 (i.e., the

controller node) includes an ISP authentication server 371. (EX1004, 22:7-11; Fig. 3B). *Freund* discloses that the authentication server 371 generates and transmits authorization instructions over the Internet: "The central authentication server checks the user's ID and password and **signals the POP server whether the user is allowed or denied access to the Internet**." (EX1004, Fig. 3B, 22:1-4, emphasis added). The signaling of the POP server whether the user is allowed or denied access to the Internet is the controller node "generating"[3] and transmitting authorization instructions to the access node. (EX1003, ¶174).

bb. Claim 19[c]: "the authorization instructions are configured to enable each of the access nodes to: receive the authorization instructions from the controller node; and"

Freund's system renders this limitation obvious. In describing the access nodes' process of receiving the authorization instructions, the '468 Patent states:

> After ICP 50 has authorized the flow of data through a CG 58, **ICP 50 may send authorization instructions to access node 66 associated with the ISP providing ISP portal 62**.

[3] The '468 Patent does not describe how authorization instructions are "generated," instead only stating that "ICP 50 may send authorization instructions to access node 66." (EX1001, 9:51-52). In that manner, the '468 Patent generates the authorization instructions by making them available, i.e., by "producing" them. (*See* EX1007).

(EX1001, 9:55-61, emphasis added). Hence, a POSA could have understood this limitation, under the broadest reasonable interpretation standard, as requiring the access nodes to be configured to receive the authorization instructions.

As discussed with respect to claim 19[b] above, *Freund* discloses the controller node generating and transmitting the authorization instructions to the access nodes. In order for the authorization instructions of *Freund* to be signaled to the POP server, it would have been obvious to a POSA to configure the POP server of *Freund* (via an initial set of authorization instructions) to enable the transfer and reception of the rest of the authorization instructions, or else the POP server would not be able to receive the entire set of authorization instructions. In other words, if the POP server uses authorization instructions transmitted from the controller node, it would have been exceedingly obvious to configure the POP server to receive the full set of authorization instructions to ensure successful communications can be completed. (EX1003, ¶¶175-178).

For example, *Freund* discloses that POPs include modems, PCs, routers, etc. (EX1004, 21:60-64), and a POSA would have been motivated, with a reasonable expectation of success, to have the central server component configure these components, via one or more instructions, with various communication configuration information (protocols, communication ports, identity verification, etc.) to facilitate efficient, robust, secure, and/or error-free communication. This

would enable the access nodes to receive the authentication instructions as claimed. For example, when communicating over the Internet (as with *Freund's* POPs and central server, *see* EX1004, Fig. 3B), TCP/IP protocols would be used, and in order to initiate communication, the POPs would be instructed with the IP address of the central server as well as the TCP port the access node should connect to. (EX1003, ¶179).

cc. Claim 19[d]: "selectively permit the gateway units to access the service provider network in accordance with the authorization instructions."

See supra Section IX(A)(1)(aa); EX1004, 22:1-6. Also, *Freund* elaborates on this process, explaining how access is granted and revoked as the situation at the client changes. (*See, e.g.*, EX1004, 22:7-41; EX1003, ¶180).

dd. Claim 23[preamble]: "A method for regulating access to a service provider network, the method comprising:"

See supra Section IX(A)(1)(a).

ee. Claim 23[a]: "generating, by a controller node coupled to the service provider network, controller instructions,"

See supra Sections IX(A)(1)(b)-(c).

ff. Claim 23[b]: "transmitting the controller instructions, by the controller node, to a plurality of gateway units of the service provider network,"

See supra Sections IX(A)(1)(d)-(e).

gg. Claim 23[c]: "receiving, by the gateway units, user-entered content requests for the service provider network,"

See supra Sections IX(A)(1)(e)-(f).

hh. Claim 23[d]: "receiving, by the gateway units, from the controller node, the controller instructions,"

See supra Section IX(A)(1)(g).

ii. Claim 23[e]: "selectively transmitting, by the plurality of gateway units, the content requests to the service provider network in accordance with the controller instructions; and transferring, by the gateway units, received content data responsive to the transmitted content requests from the service provider network."

See supra Sections IX(A)(1)(h)-(i).

jj. Claim 24[preamble]: "The method of claim 23"

See supra Sections IX(A)(1)(dd)-(ii).

kk. Claim 24[a]: "further comprising storing the controller instructions, by the gateway units, in storage devices of the gateway units,"

See supra Sections IX(A)(1)(k).

ll. Claim 24[b]: "wherein each of the gateway units has an identifier that uniquely identifies the gateway unit."

See supra Sections IX(A)(1)(l).

mm. Claim 25: "The method of claim 23, further comprising the gateway nodes denying access to a first group of network servers of the service provider network, in accordance with the controller instructions."

Claim 25 refers to "***the*** gateway nodes" (emphasis added), which does not have an antecedent basis. Claim 23 only refers to gateway units. To the extent that the term "gateway nodes" is intended to mean "gateway units," as discussed above, *Freund* renders obvious this claim. (*See supra* Sections IX(A)(1)(dd)-(ii) and (m)-(n)). If "gateway nodes" is not intended to mean "gateway units," then it is unclear what this term means. (EX1003, ¶190).

nn. Claim 26: "The method of claim 25, further comprising the gateway nodes notifying the controller node if a content request designates a network server of the service provider network."

See supra Section IX(A)(1)(mm). To the extent "gateway node" means "gateway unit," *Freund* renders obvious this claim. (*See supra* Sections IX(A)(1)(dd)-(ii) and (o)-(p); EX1003, ¶191).

oo. Claim 27: "The method of claim 25, further comprising the gateway nodes detecting a content request that designates a first network server of the service provider network; and re-directing the content request to a second network server of the service provider network."

See supra Section IX(A)(1)(mm). To the extent "gateway node" means "gateway unit," *Freund* renders obvious this claim. (*See supra* Sections IX(A)(1)(mm) and (q)-(s); EX1003, ¶192).

pp. Claim 33[preamble]: "The method of claim 23,

See supra Sections IX(A)(1)(dd)-(ii).

qq. Claim 33[a]: "further comprising a gateway unit receiving registration information from a user via a user interface of the gateway unit;

See supra Sections IX(A)(1)(u)-(v).

rr. Claim 33[b]: "transmitting the registration information to the controller node;"

See supra Sections IX(A)(1)(b)-(c).

ss. Claim 33[c]: "and on registration, receiving initial operating parameters from the controller node."

See supra Section IX(A)(1)(x).

B. Ground 2: *Spusta* Renders Claims 1-3, 11, 13, 23-25, 32, and 34 Obvious

This ground relies on *Spusta* and is meaningfully distinct from Ground 1, which relies on *Freund.*

Freund and *Spusta* address similar issues in the field of networking, including managing, regulating, and restricting access to network content. However, while they may disclose similar functions generally, their respective systems and methods are configured in different ways. For example, while *Freund* discloses, in part, a "client-based filter application" featuring an entire suite of rules available for use in access management (e.g., time limits, permitted application, permitted URLs, permitted protocols, etc.; *see* EX1004, 4:5-28),

Spusta discloses a simpler system and method that is, in part, a "browser system" focused on filtering websites and age-appropriate content based on database entries (*see* EX1005, ¶¶ 52-54).

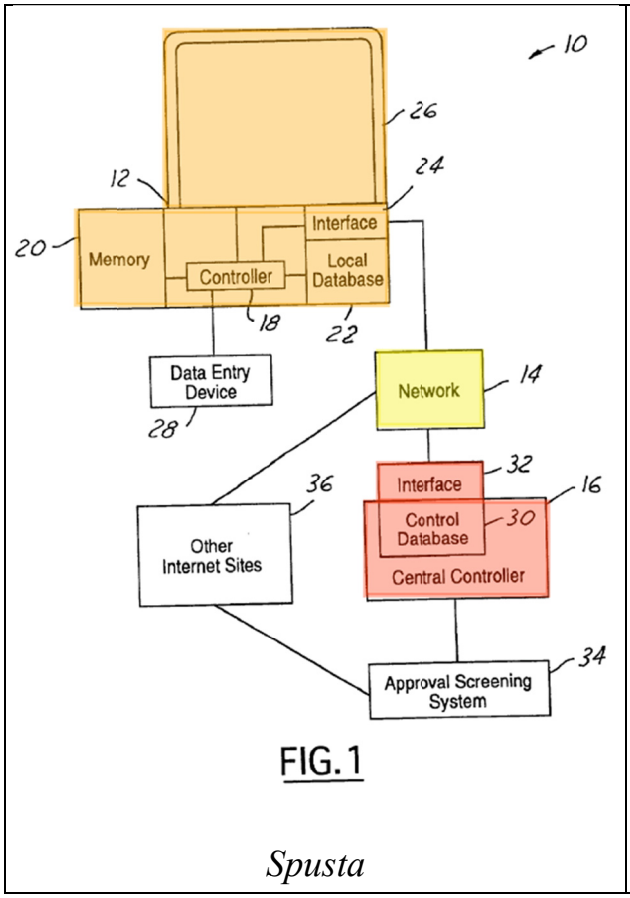
As Patent Owner may attempt to distinguish elements of the challenged claims based upon purportedly unique claim features, which are clearly described by each of *Freund* and *Spusta*, both grounds should be included for trial.

1. *Spusta*

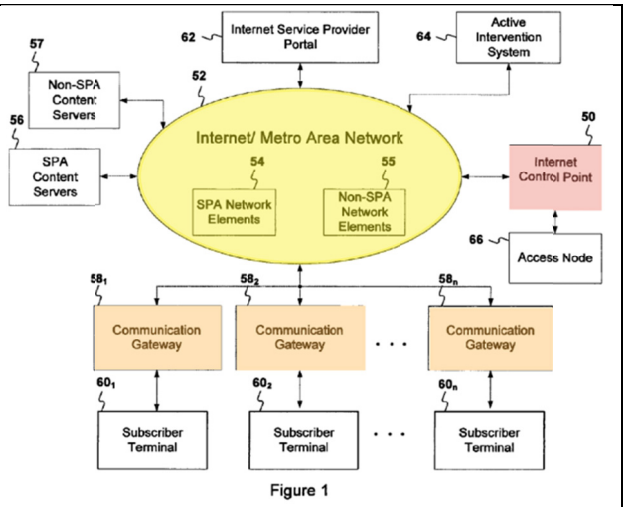
Spusta is directed to regulating network access and describes a web browser system with a local database on a local computer and a central database on a central controller. The database entries include instructions to allow access to a particular domain name. (EX1005, Abstract). When changes are detected, instructions are sent from the central controller's database to the local computer's database. These instructions direct the local computers (gateway units) to either allow or deny access to network servers in response to client-issued requests. The instructions can also direct the local computers to display a start-up page appropriate for the current user or to display advertising selected for the current user. (EX1005, ¶¶[0008], [0050], [0060], Figs. 3, 5, 10; EX1003, ¶50).

Spusta's architecture is shown in annotated Fig. 1 (below, left), which is also virtually indistinguishable from the '468 Patent's architecture when shown side-by-side (below, right). Highlighted are the client computers (i.e., the claimed

"gateway units") in orange, the controller in red, and the network (i.e., the network to which access is to be controlled) in yellow. (EX1003, ¶¶51, 75-77).



Spusta



The '468 Patent

a. Claim 1[preamble]: "A system for regulating access to a service provider network, the system comprising,"

Spusta discloses a system for regulating access to the Internet (i.e., a service provider network):

> The present invention provides an improved browser system … When the domain name is in the local database or central database, access to the ***website*** is enabled.

(EX1005, ¶[0008] (emphasis added)).

> Referring now to FIG. 1, a browser system 10 according to the present invention is illustrated. Browser system 10 has a local computer 12 that is coupled to a network 14. Network 14 is coupled to a remote or central controller 16. Network 14 may, for example, be one of a number of various types of connections to the Internet…
>
> "Central" or "remote" when describing controller or database refers to the device or database being located away from or separated from the local computer by the network 14.

(EX1005, ¶[0049]; EX1003, ¶81). *Spusta* thus discloses that the network can include the Internet and can include intended destinations such as domain name, website address, and URL. (EX1005, ¶[0048-0049]). As depicted in Fig. 1, network 14 provides connectivity to components that could not otherwise communicate, such as local computer 12, central controller 16, and other internet sites 36.

Accordingly, *Spusta* discloses a browser system that is coupled to the Internet, and provides a system for regulating access to a service provider network. (EX1005, title) ("Web browser for limiting access to content on the Internet.") (EX1003, ¶81-82).

b. Claim 1[a]: "a controller node coupled to the service provider network,"

Annotated Fig.1 below shows that *Spusta* discloses a controller node coupled to the service provider network.

Spusta explains that "[n]etwork 14 is coupled to a remote or ***central controller 16***," which, in conjunction with local computers, performs monitoring and filtering. (EX1005, ¶[0049] (emphasis added)). The central controller, shown in red, is connected to the network, shown in yellow.

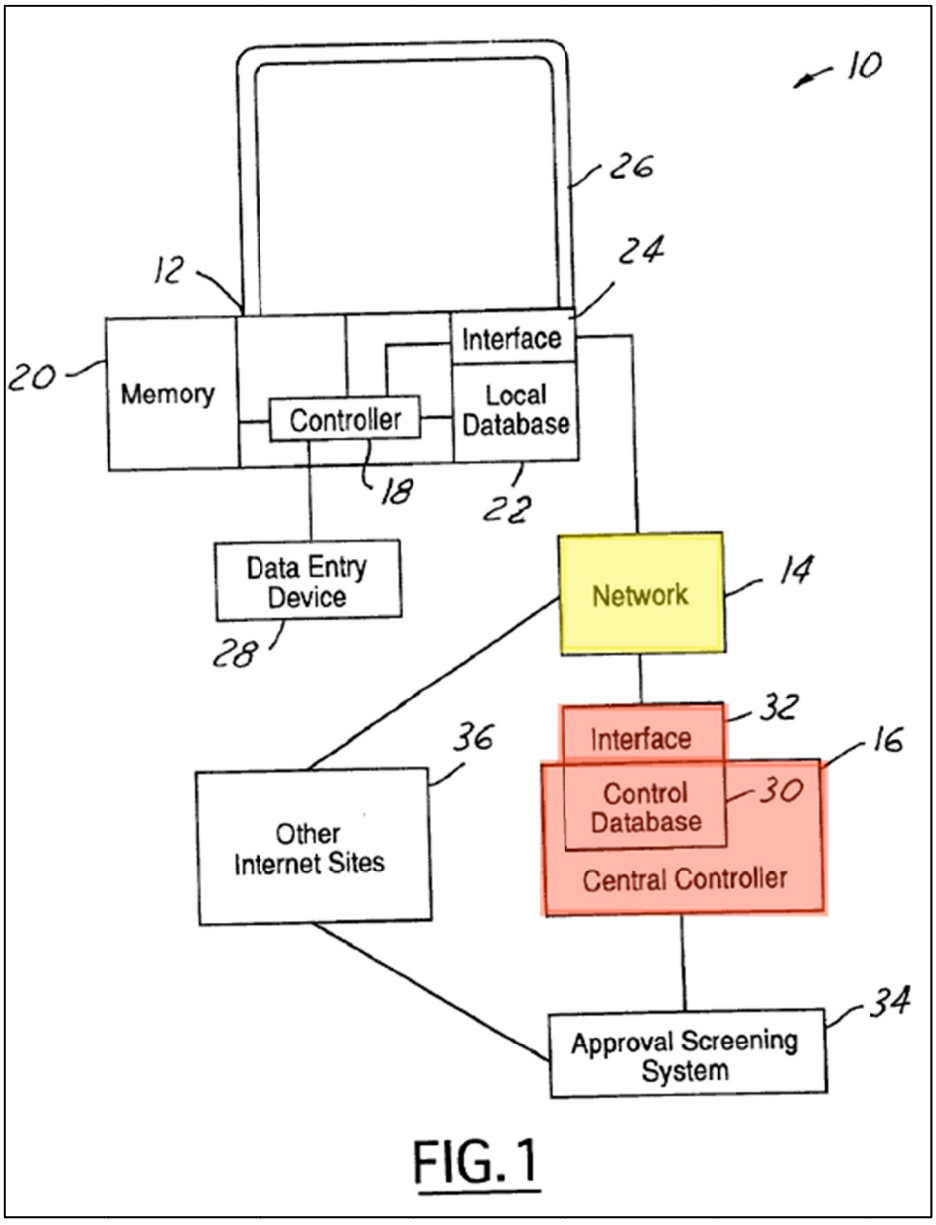


FIG. 1

Spusta also explains that "[c]entral controller 16 may be one or a plurality of

computers or servers used to store a central database 30 which may be coupled to network 14 through an interface 32." (*See supra* Section VIII(A); EX1005, ¶[0053]; EX1003, ¶85).

c. Claim 1[b]: "the controller node comprising a first processor configured to generate controller instructions, and"

Spusta discloses a first processor. Central controller 16 (the claimed "controller node") is a "device" and is "one or a plurality of computers or servers." (EX1005, ¶¶ [0049], [0053]). A POSA would have recognized that a claimed "first processor" is necessarily present in any of the computers and servers. Nevertheless, even if one were to argue that computers and servers do not necessarily have processors, a POSA would have been motivated to (and found it exceedingly obvious to) include a processor to provide the ability to execute code, access the control database, communicate with network 14, and execute all the other operations that are performed by the central controller and would have had a reasonable expectation of success in doing so. (EX1005, ¶[0053], Fig. 1; *see also infra* Section IX(B)(1)(d); EX1003, ¶91).

Spusta also discloses the first processor configured to generate controller instructions. As discussed above, "controller instructions" include "information that is sent by the controller that is used to direct the actions of a network unit," such as URLs. (*See supra* Section VIII(B)). *Spusta* explains that "central

controller 16 has a central database 30" that "may contain various information about each approved website." (EX1005, ¶[0092]). *Spusta* goes on to explain that the instructions include information including a "URL" which "represents the parsed domain name determined in the parsing steps of Fig. 4" and a "status field" which "determines whether the domain name is approved, denied or pending." (EX1005, ¶[0092]). These database entries with URLs used to approve or deny access to particular domain names constitute the claimed "controller instructions." Annotated Fig. 11 below highlights how these instructions are stored. (EX1003, ¶92).

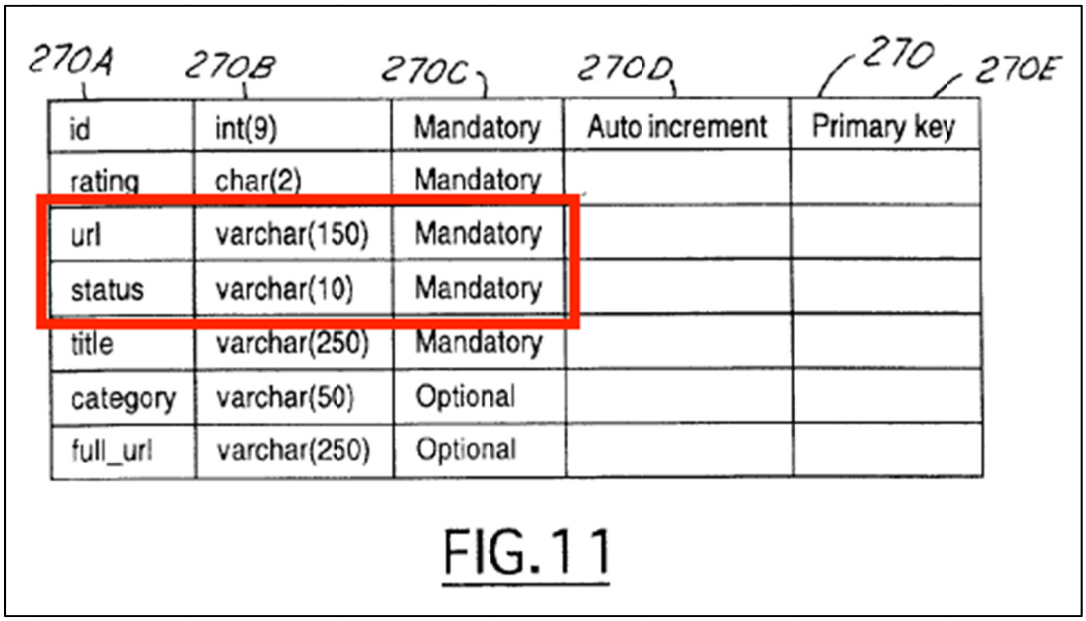


FIG. 11

Annotated Fig.1 below highlights the central database within the central controller. (EX1003, ¶93).

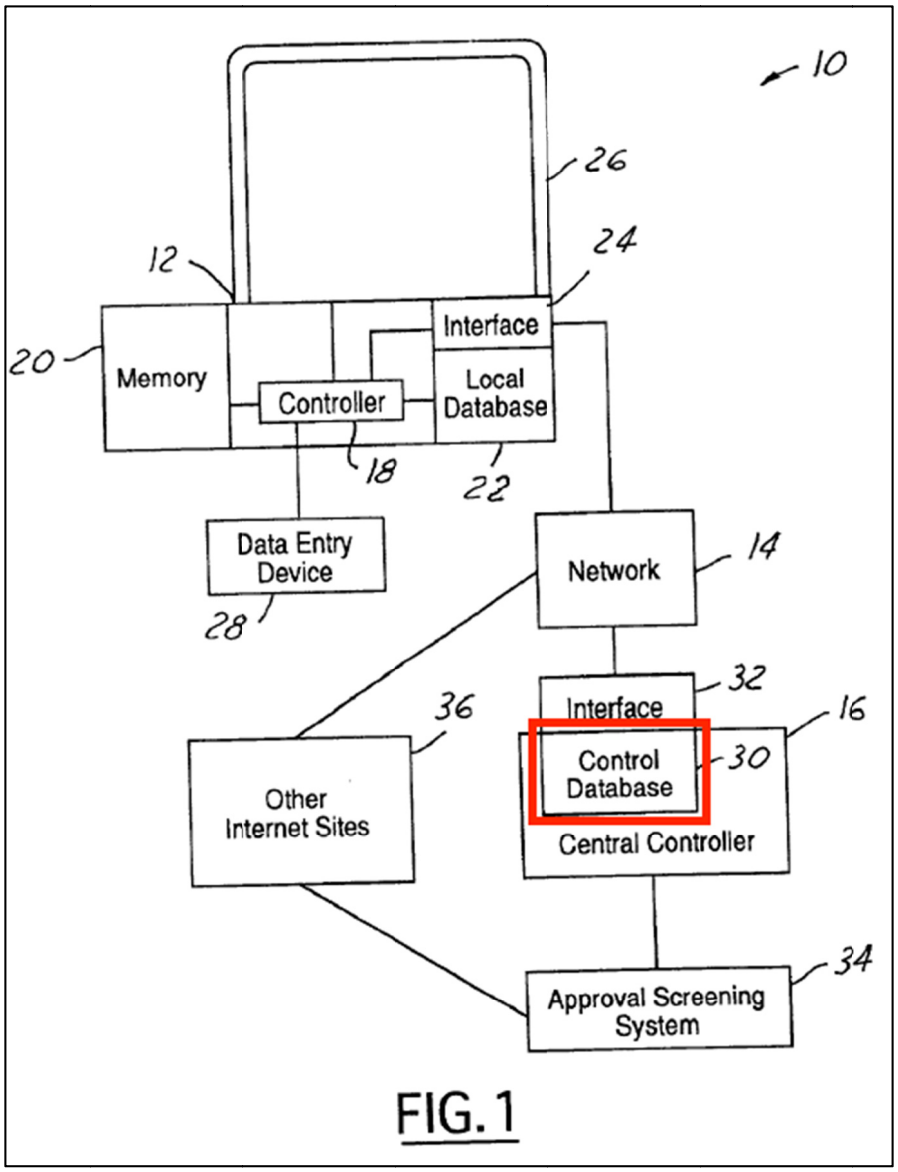


FIG. 1

Additionally, *Spusta* discloses, with reference to Fig. 13, that "because Internet information changes nearly constantly, the system of the present invention allows approved websites to be monitored and their status changed," which causes updated instructions to be generated. (EX1005, ¶[0095]). For example, "[i]n step 288, if it is determined that the website has changed and inappropriate content is acquired, step 290 is performed wherein the central database is changed."

(EX1005, ¶[0095]). The annotated Fig. 13 below shows the process by which the central database is updated (or changed), which generates controller instructions to reflect those updates. (EX1003, ¶94).

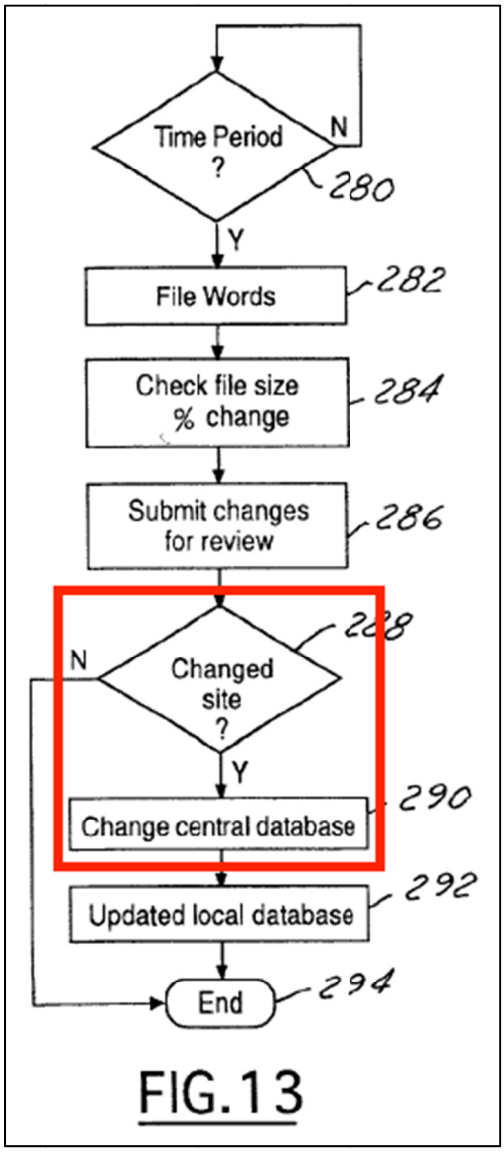


FIG. 13

After the central database is updated in step 290, in step 292, shown above, the local databases at the local computers are also updated. A POSA would have understood that *Spusta's* database contains controller instructions because the

database contains information that is used to direct the actions of a local computer, (the claimed "gateway unit"). (EX1003, ¶95).

d. Claim 1[c]: "the controller node comprising … a first network interface configured to transmit the controller instructions over the service provider network to a plurality of gateway units; and"

As shown in annotated Fig. 1 below, *Spusta* discloses a first network interface 32, shown in purple, configured to transmit the database entries (i.e., the claimed "controller instructions") over network 14 (the claimed "service provider network") to a plurality of local (or user) computers 12 (i.e., the claimed "gateway units"), shown in orange below. (EX1003, ¶104).

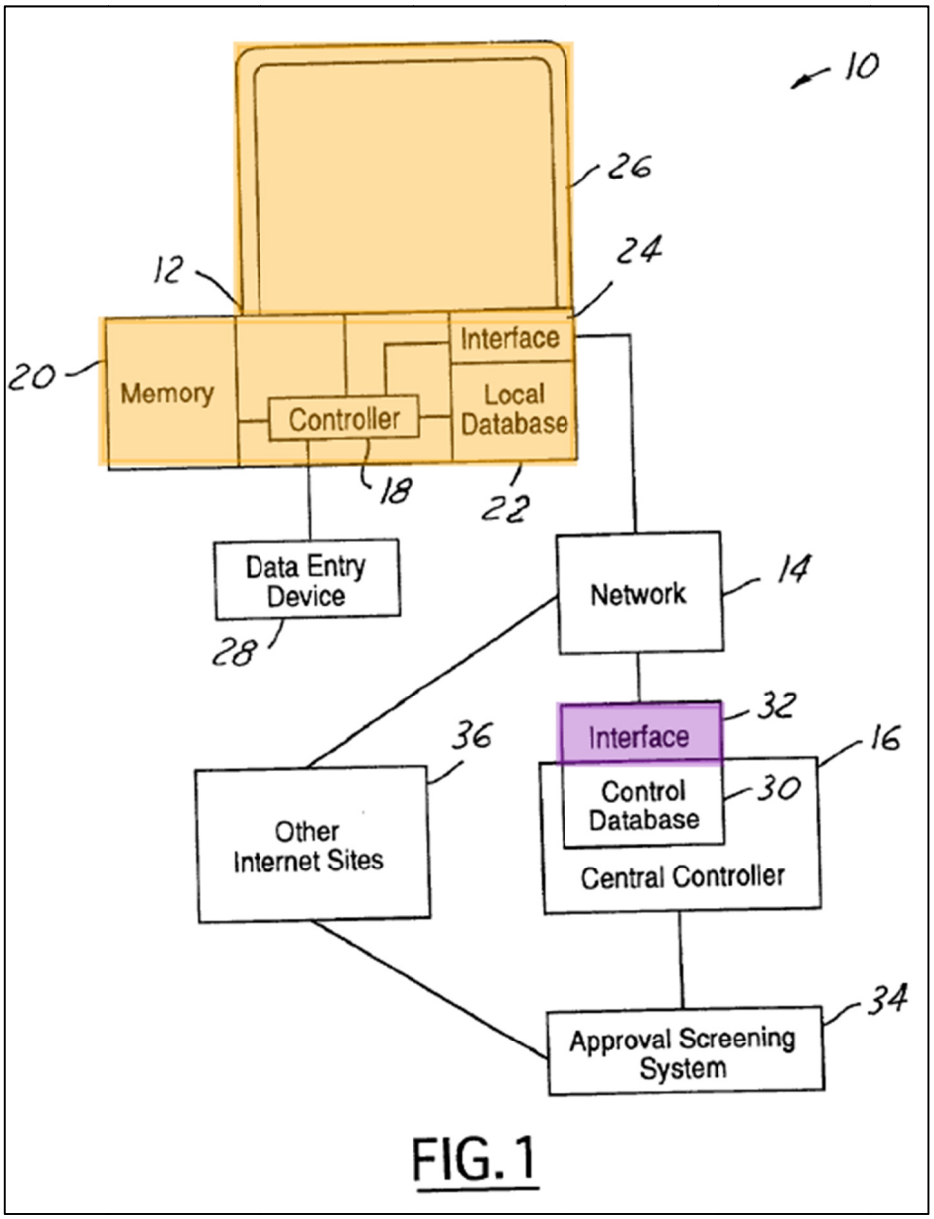


FIG. 1

Spusta discloses that central controller 16 is "used to store a central database 30 which may be coupled to network 14 through an interface 32." (EX1005, ¶[0053]). *Spusta* further discloses that "[c]entral database 30 has central database entries" that can include the information shown in Fig. 11 below, such as portions of URL names. (EX1005, ¶¶[0053], [0092]). This information is sent to the local

computers (the claimed "gateway units") in a variety of circumstances. For example, if a website name (name1) is found in the central database and not in the local database then "a new table entry containing the desired data" is added to the local database. (EX1005, ¶¶[0065]-[0070]).

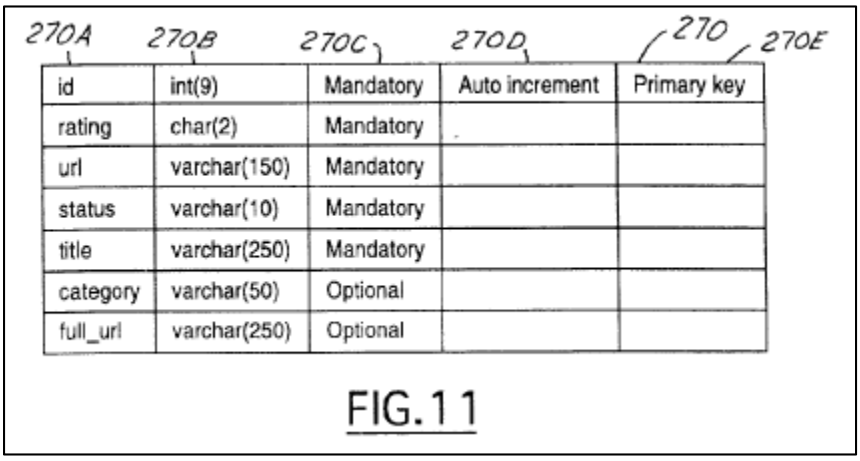


FIG. 11

(*See also supra* Section IX(B)(1)(c); Fig. 13; ¶[0095] ("After step 290, the local databases must also be updated. The local databases are updated when the user logs in to the central database. A change will remove the website from the approved list of the local database upon log in.")). And, while Fig. 1 of *Spusta* depicts a single local computer 12, *Spusta* explains that "various numbers of local computers 12 are contemplated by the present invention." (EX1005, ¶[0049]; EX1003, ¶105; *see also infra* Section IX(B)(1)(e)).

e. Claim 1[d]: "the plurality of gateway units,"

Spusta discloses a plurality of local (or user) computers 12 (i.e., the claimed "gateway units"), each of which control access to the network. *Spusta* explains

that "[t]he present invention provides an improved browser system that includes a network that connects a user computer having a local database with local database entries therein with a central database having central database entries therein." (EX1005, ¶[0008]). *Spusta's* annotated Fig. 1 below shows the local computer 12 in orange. (EX1003, ¶108).

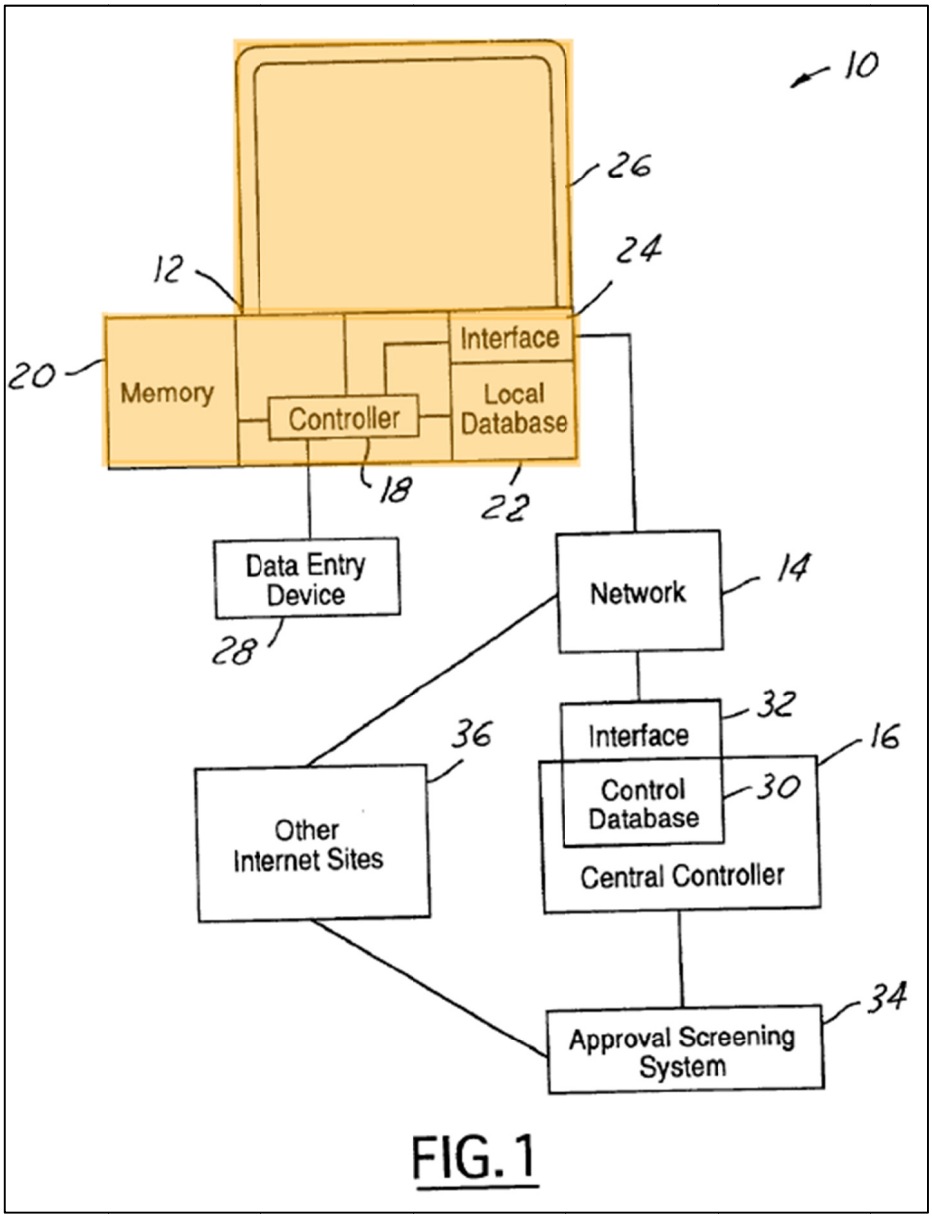


FIG. 1

Spusta explains that:

> Local computer 12 has a local controller 18 that is microprocessor based. Controller 18 controls the operation of local computer 12 and the operation of a memory 20, a local database 22, a network interface 24, and a display 26…. Memory 20 stores the software to run the web browser in response to data entry device 28.

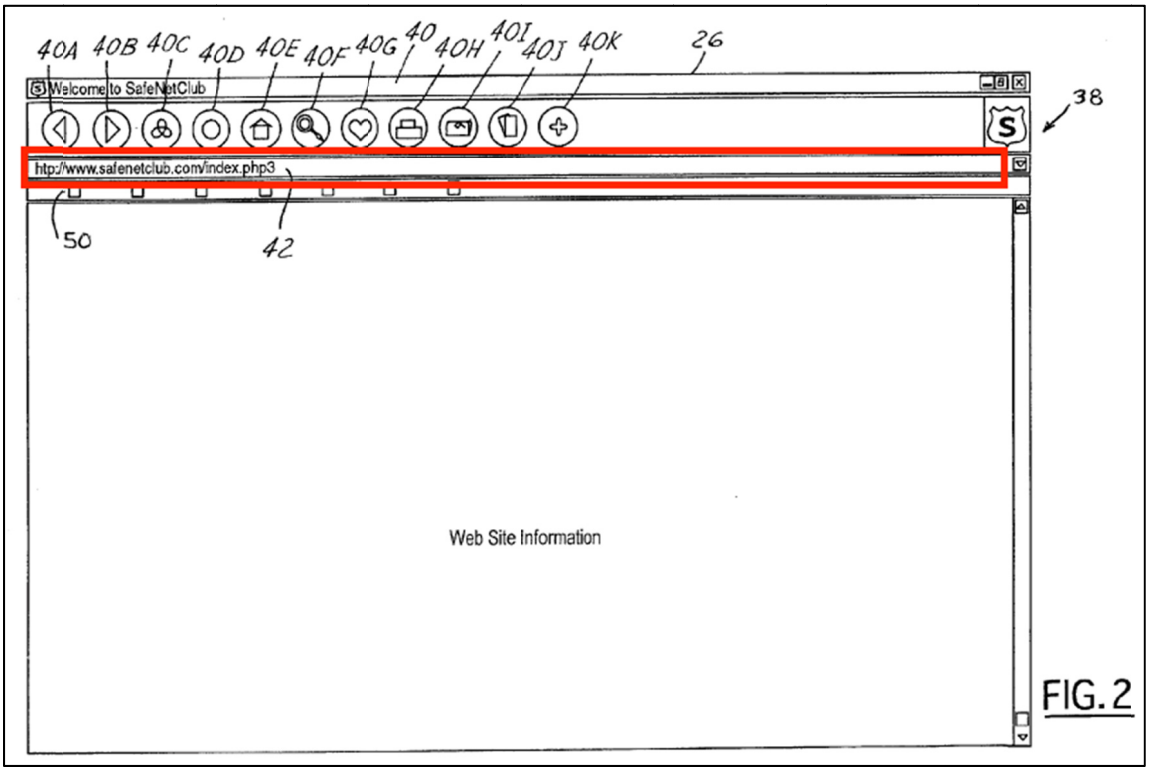
(EX1005, ¶[0050]). *Spusta* further discloses a plurality of local computers so configured, "[a]lthough only one local computer 12 is illustrated, various numbers of local computers 12 are contemplated by the present invention." (EX1005, ¶[0049]; EX1003, ¶109).

f. Claim 1[e]: "each of the plurality of gateway units comprising: a user interface configured to receive user-entered content requests for the service provider network,"

Spusta discloses a browser system and/or data entry device (i.e., the claimed "user interface") configured to receive user-entered content requests for the service provider network. (EX1005, title) ("Web browser for limiting access to content on the Internet."). *Spusta* discloses both a hardware and a software "user interface." (EX1003, ¶113).

Spusta discloses a software user interface (a web browser) that allows the local computer (i.e., the claimed "gateway unit") to receive network requests entered by subscribers: "A web browser has a domain name entry area for entering

a domain name corresponding to the website." (EX1005, ¶[0008]). This is shown in *Spusta's* annotated Fig. 2 below. (EX1003, ¶114).



Spusta explains that "[d]isplay 26 displays a browser 38, which is a graphical user interface." (EX1005, ¶[0055]). "A website URL address display 42 is used to display the current website as well as enter a requested website to be navigated to." (EX1005, ¶[0056]; EX1003, ¶115).

Spusta also discloses a hardware user interface, including a display and data entry devices common on PCs, shown in blue below.

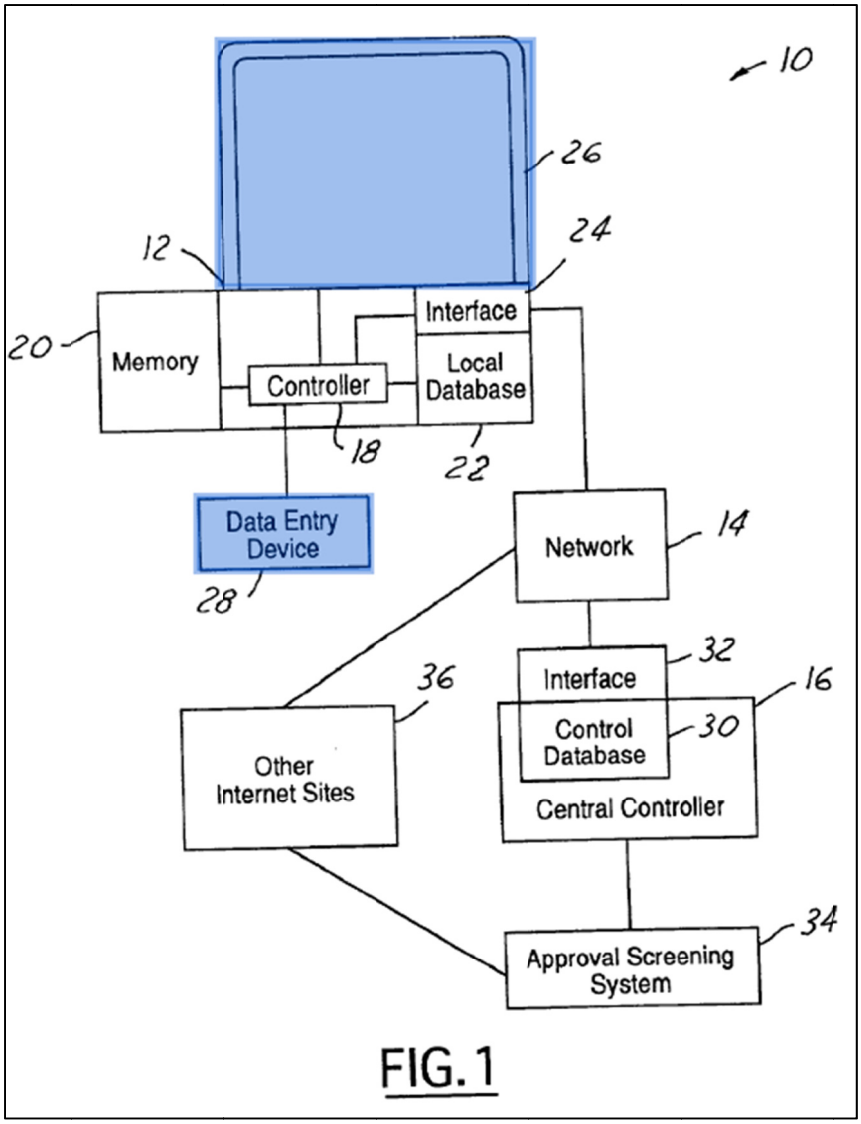


FIG. 1

Spusta explains that "[l]ocal computer 12 has … a display 26. … Memory 20 stores the software to run the web browser in response to data entry device 28." (EX1005, ¶[0050]; EX1003, ¶116).

g. Claim 1[f]: "each of the plurality of gateway units comprising … a second network interface coupled to the service provider network and configured to receive the controller instructions from the controller node through the service provider network"

In annotated Fig. 1 below, *Spusta* discloses a second network interface 24, shown in gray below, coupled to the service provider network 14 and configured to receive the database entries (i.e., the claimed "controller instructions") from the central controller 16 (i.e., the claimed "controller node") through the service provider network. (EX1003, ¶119).

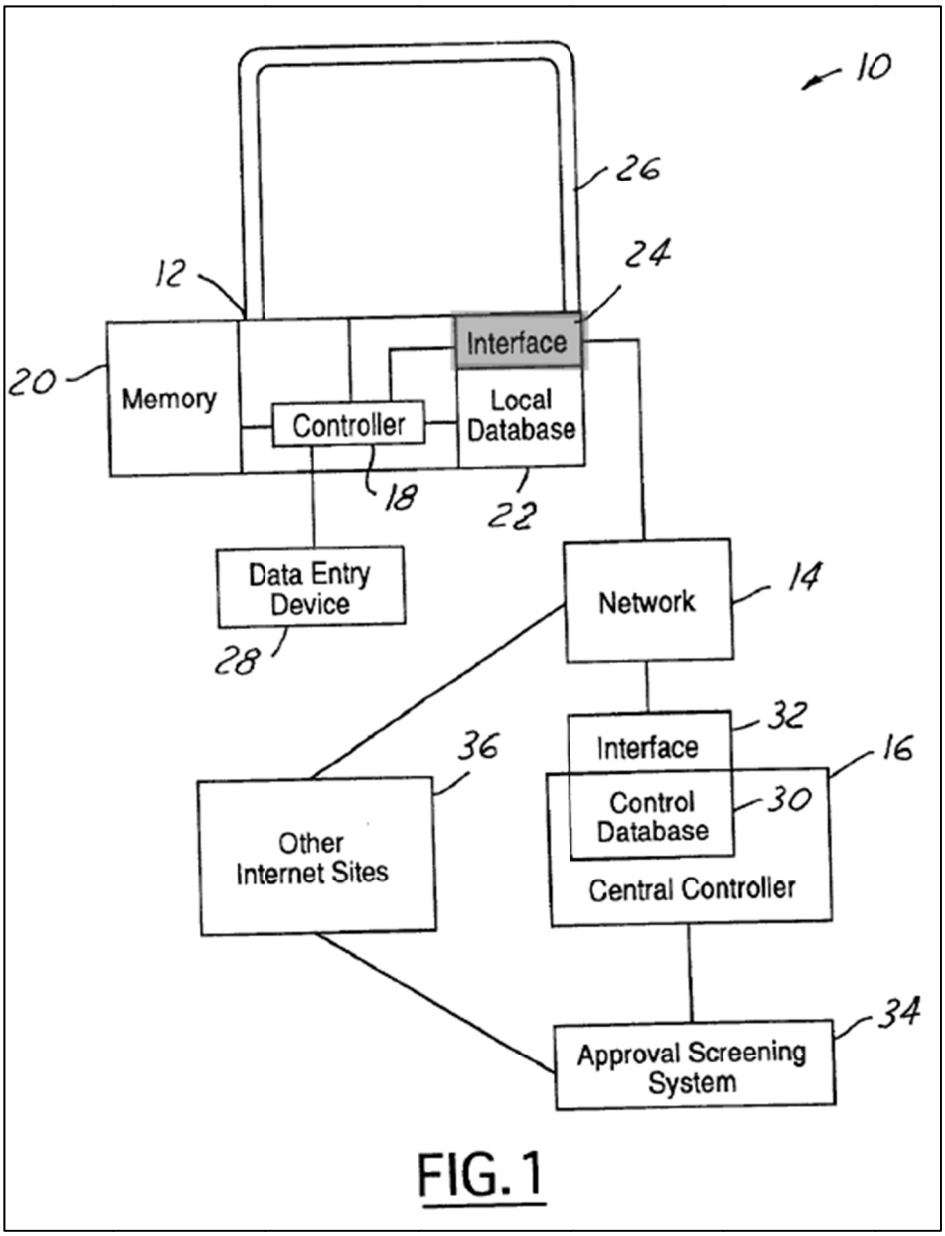


FIG. 1

Spusta discloses that "[l]ocal computer 12 has … a network interface 24." (EX1005, ¶[0050]). This network interface receives database entries from central controller 16 over network 14.

For example, with reference to Fig. 5, *Spusta* discloses that when a database entry exists in the central database (i.e., the database of the controller) but not in

the local database (i.e., the database of the user computer), then the database entry is copied from the controller to the local computer (see red highlight in Fig. 5):

> [I]f name2 was found in the central database (and name1 was not found in the local database) then name2 is stored in the local database in step 143, then step 146 is executed. This may be performed by adding a new table entry containing the desired data into the local database. The entry may be all or part of the tables described below which is transferred through the network.

(EX1005, ¶[0068]; EX1003, ¶120).

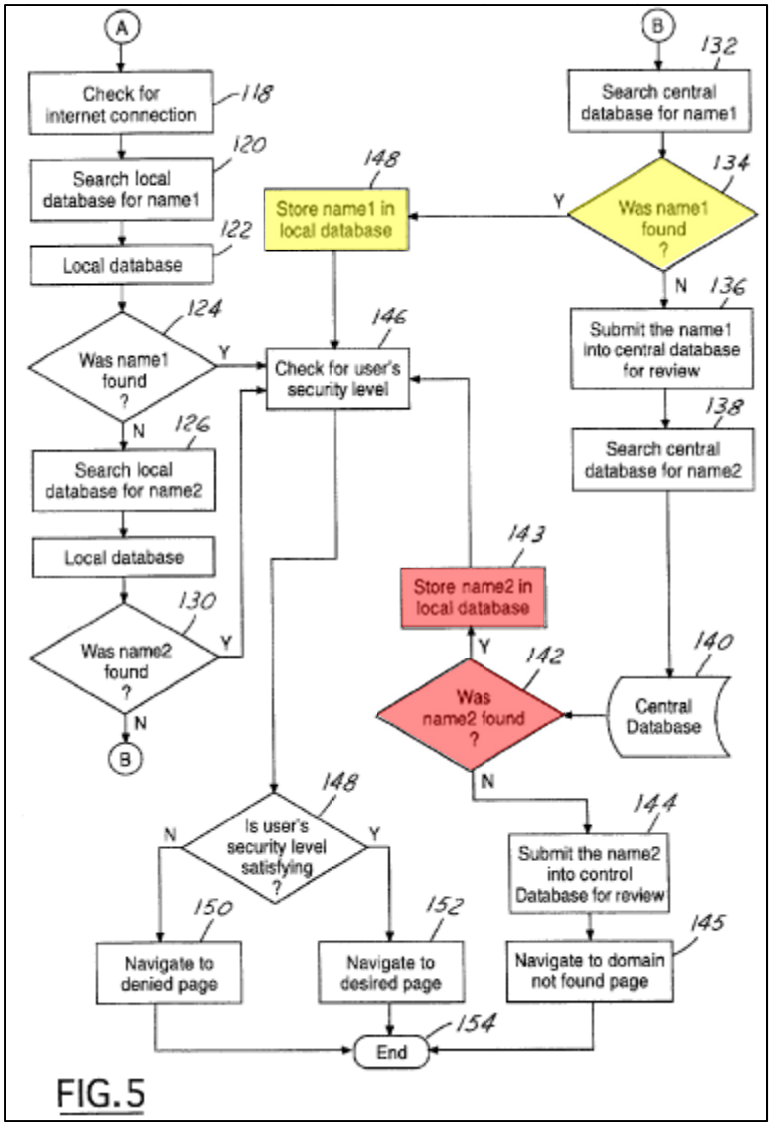


FIG.5

In another example, *Spusta* explains that "[r]eferring back to step 134, if name1 was found in the central database (not found in the local database) step 148 is executed. In step 148 name1 is stored in the local database in the same manner described above." (EX1005, ¶[0069], Fig. 5 (see yellow highlight above)).

Furthermore, in yet another example referring to Fig. 13 below, *Spusta* discloses that the local database is updated when the central database is changed:

[S]tep 290 is performed wherein the central database is changed. After step 290 the local databases must also be updated. The local databases are updated when the user logs in to the central database. A change will remove the website from the approved list of the local database upon log in.

(EX1005, ¶[0095]; EX1003, ¶121).

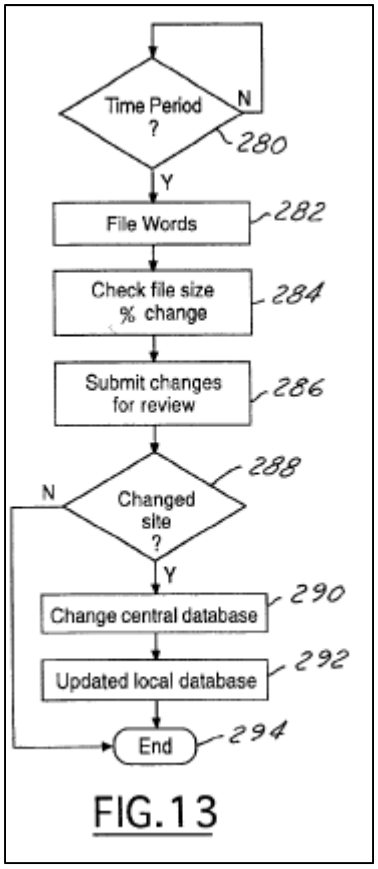


FIG.13

h. Claim 1[g]: "each of the plurality of gateway units comprising … a second processor coupled to the user interface and the second network interface"

Spusta discloses a controller 18 (i.e., the claimed "second processor"), shown in pink below, coupled to the browser system and/or data entry device (i.e.,

the claimed "user interface") and interface 24 (the claimed "second network interface").

As explained in claim 1[e], *Spusta* discloses several instances of the user interface, including software user interfaces (e.g., browser 38, which is a graphical user interface, is stored in memory 20, and is run in response to data entry device 28) and hardware user interfaces (e.g., display 26, data entry device 28). (EX1005, ¶¶[0008]. [0050], [0055], [0056]). As shown by the connections in annotated Fig. 1 below, *Spusta's* user interfaces are each coupled to the second processor (controller 18, in pink below). (EX1003, ¶125).

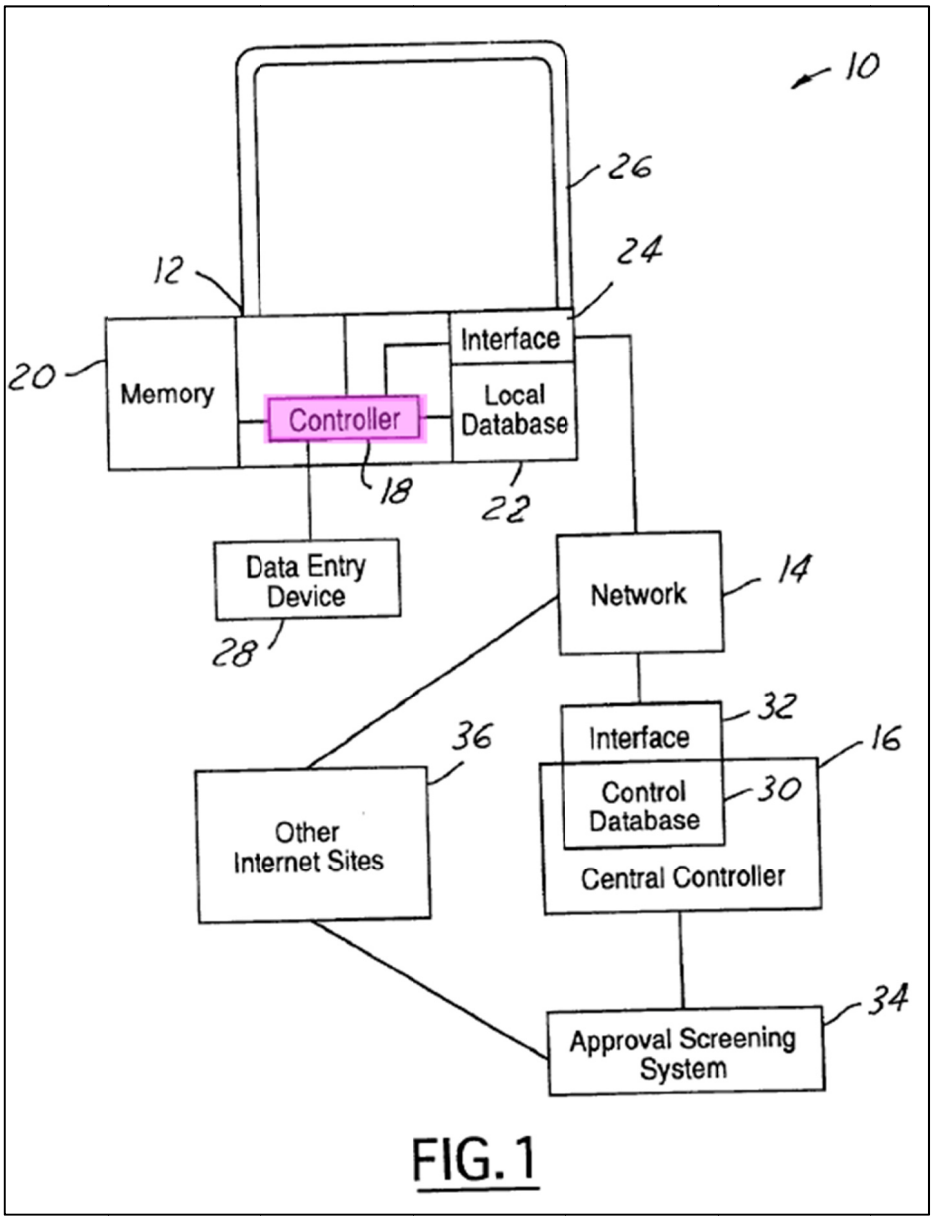


FIG. 1

As also shown in Fig. 1 above, the second processor (controller 18, in pink), is coupled to the second network interface (interface 24).

Spusta explains that the second processor (controller 18) is "microprocessor based" and "controls the operation of local computer 12 and the operation of a

memory 20, a local database 22, a network interface 24, and a display 26." (EX1005, ¶[0050]). (EX1003, ¶¶126-128).

i. Claim 1[h]: "wherein the second processor is configured to selectively transmit the content requests to the service provider network in accordance with the controller instructions, and transfer received content data responsive to the transmitted content requests from the service provider network via the second network interface."

Spusta discloses this element in a series of steps of an approval process determining whether access to Internet content is to be limited.

Spusta discloses that a " navigation process is initiated by a user typing in (for example in URL display 42 of FIG. 2) or selecting a desired URL (Uniform Resource Locater)." (EX1005, ¶[0062]). This content request is subject to an approval process performed on the gateway units (local computer 12) as shown in the annotated Fig. 5 below. (EX1003, ¶133).

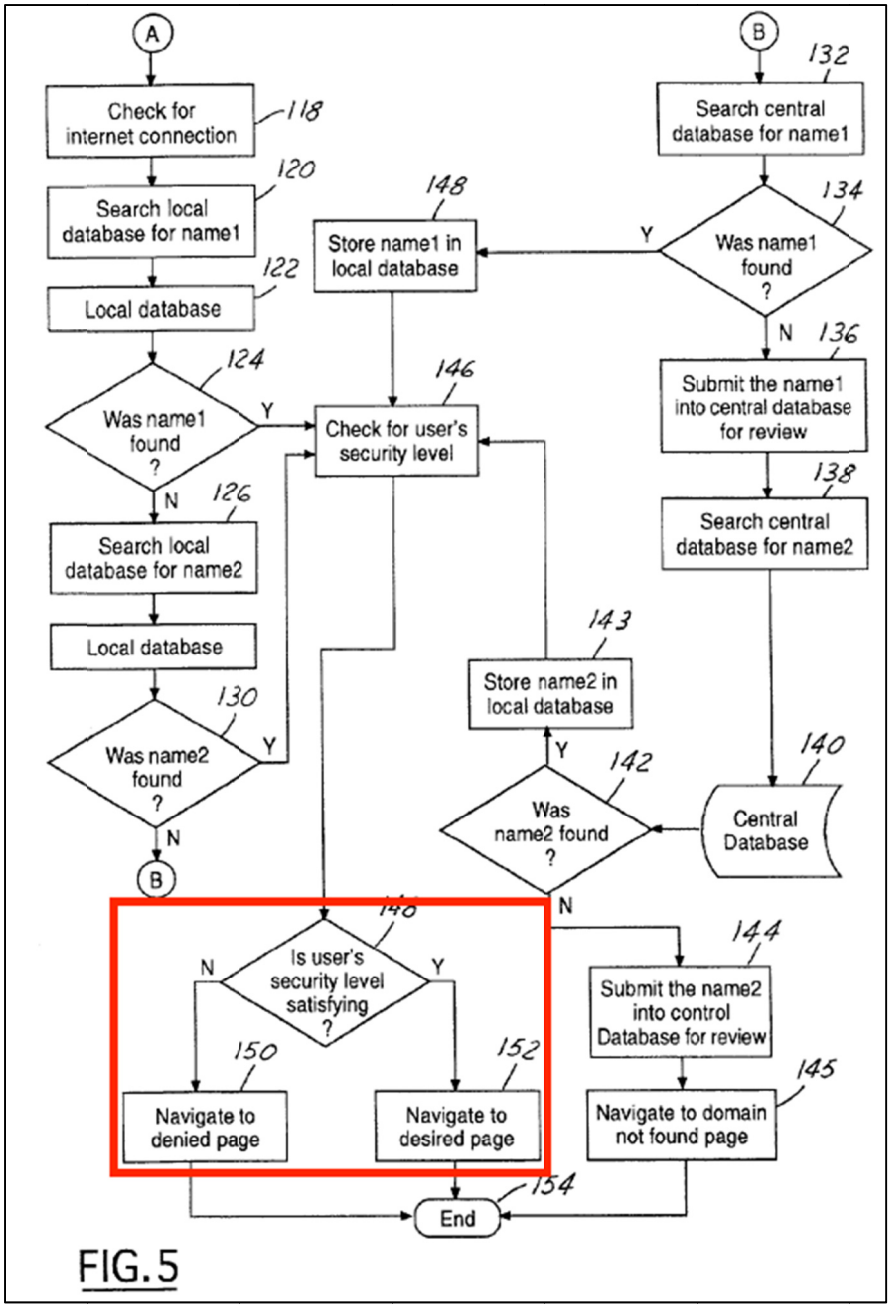


FIG. 5

Spusta describes the approval process which is applied to each content request. First, the URL entered by the user is parsed into appropriate formats for processing (e.g., into "name1" and "name2" formats, *see* EX1005, ¶[0062]-[0064]). Then, the controller instructions are consulted:

> In step 120, the local database on the local computer is searched for name1. If name1 was not found in the local database in step 124, step 126 is executed in which name2 is searched for in the local database in step 128. It should be noted that "found," "not found," and "within" when referring to the database refer to whether or not the site is approved. Thus, when a website name is "found," it is envisioned that it is on the "approved" (accessible) list of sites. The database may actually contain information on disapproved sites as well.

(EX1005, ¶[0065]). *Spusta* explains that if, for example, neither name1 nor name2 were found in the local database or the central database, further navigation to the desired site is prevented. (EX1005, ¶[0067], Fig. 5; EX1003, ¶134).

If, on the other hand, name1 and/or name2 were found in the local database (e.g., meaning that the URL is an accessible site), an additional security level check is performed in accordance with the controller instructions.

> In step 146, the user's security level is checked. This may correspond to the grade levels of children described above. After step 146, step 148 is executed in which the user's security level is determined whether or not it satisfies the particular level of the website. **Thus, a comparison is made between a database entry indicating level and the level of the current user.** If the site has a security level beyond that of the website, then step 150 is executed in which access to or navigation to the website is denied. In step 148 if the user's security level is greater than or corresponds with the security level of the website, then the navigation is allowed to the website.

(EX1005, ¶[0070], emphasis added; *see supra* Section VIII(B); EX1003, ¶133).

When navigation to the website is allowed in step 148, a POSA would have understood that this means that the content of that website is received by the local computer 12 from network 14 under the control of the controller 18 (the claimed "second processor") via interface 14. (EX1003, ¶134; *see supra* Sections IX(C)(1)(c)-(e), (g), and (h); EX1005, Fig. 1).

j. Claim 2[preamble]: "The system of claim 1 wherein,"

See supra Sections IX(C)(1)(a)-(i).

k. Claim 2[a]: "each of the gateway units further comprises a storage device configured to store the controller instructions; and"

In annotated Fig. 1 below, *Spusta* discloses that each of the local computers 12 (i.e., the claimed "gateway units") further comprises a storage device, shown in light blue below, configured to store the database entries (i.e., the claimed "controller instructions").

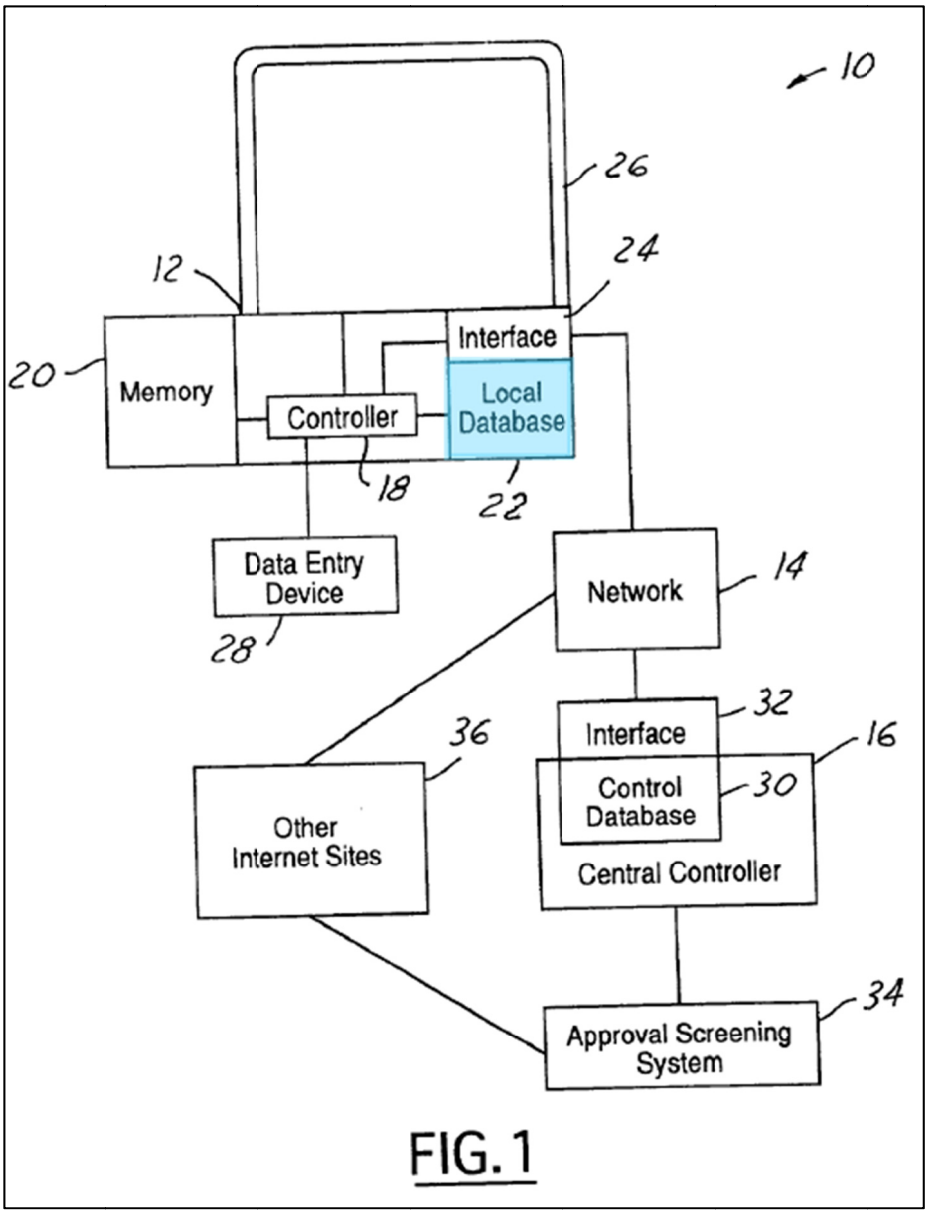


FIG. 1

As discussed in claim 1[f] above, *Spusta* discloses the gateway units receiving the controller instructions in its local database 22. Further, to the extent *Spusta* may not explicitly describe that the local database 22 is a "storage device," *Spusta* further explains that "[a]lthough memory 20 and local database 22 are illustrated as separate components, these components may be combined into a single memory 20." (EX1005, ¶[0050]; EX1003, ¶137).

l. Claim 2[b]: "each the gateway units has an identifier that uniquely identifies the gateway unit."

It would have been known to a POSA that each of *Spusta's* local computers (i.e., the claimed "gateway units") would necessarily have an identifier that uniquely identified it because since the 1990's, as computers were connected to a network, each computer has had a number of identifiers that uniquely identify that computer. These include names, Ethernet MAC (Media Access Control) addresses, and IP (Internet Protocol) addresses. Additionally, every networked local computer has at least an IP address which uniquely identifies that computer and that such an identifier is necessarily there to enable communications.

Moreover, even if it were possible to implement *Spusta*'s system without an identifier, it would have been obvious for a POSA to add one, like all networked computers, to facilitate network communication with specific and identifiable units, and a POSA would have had a reasonable expectation of success. (EX1003, ¶140).

m. Claim 3[preamble]: "The system of claim 1"

See supra Sections IX(C)(1)(a)-(i).

n. Claim 3[a]: "wherein the controller instructions include instructions configured to deny access to a first group of network servers of the service provider network."

Spusta discloses that the database entries (i.e., the claimed "controller instructions") include entries configured to deny access to a first group of network

servers of the service provider network. *Spusta* discloses that there are a number of circumstances where access to particular network servers is denied. A first circumstance is when "name1 or name2 was not found in either the local database or the central database. Therefore, step 144 issues a domain not found page 145 and prevents the further navigation to the desired site." (EX1005, ¶[0067]). Accordingly, *Spusta* discloses denying access to a first group of network servers, or websites, of the service provider network because the first group of network servers are not found in the databases as approved sites. (EX1003, ¶143).

And, when the network server *is* found as approved in either the local or the remote database, *Spusta* discloses a second circumstance under which navigation is denied to websites based on a user's (such as a grade student's) security level in a database entry. (EX1005, ¶[0070]; EX1003, ¶151). Accordingly, a POSA would have understood that *Spusta's* database includes database entries that are configured to deny access to a first group of network servers, or websites, of the service provider network because *Spusta* denies access to all websites greater than the user's security level. For example, children of lower grades would be shielded from all web sites containing graphic material. (EX1003, ¶¶143-144).

Third, *Spusta* discloses that the database entries can be configured to deny access to a first group of network servers of the service provider network by explicitly listing the disapproved sites. (EX1005, ¶[0065]; EX1003, ¶145).

o. Claim 11: "The system of claim 1, wherein the controller instructions include a pre-determined network site, and the controller instructions are configured to cause a gateway unit to access the predetermined network site upon initiation of network browser software on the gateway unit."

In annotated Fig. 3 below, *Spusta* discloses that the database entries (i.e., the claimed "controller instructions") can include a pre-determined network site, and database entries are configured to cause a local computer (i.e., the claimed "gateway unit") to access the predetermined network site upon initiation of network browser software on the user computer.

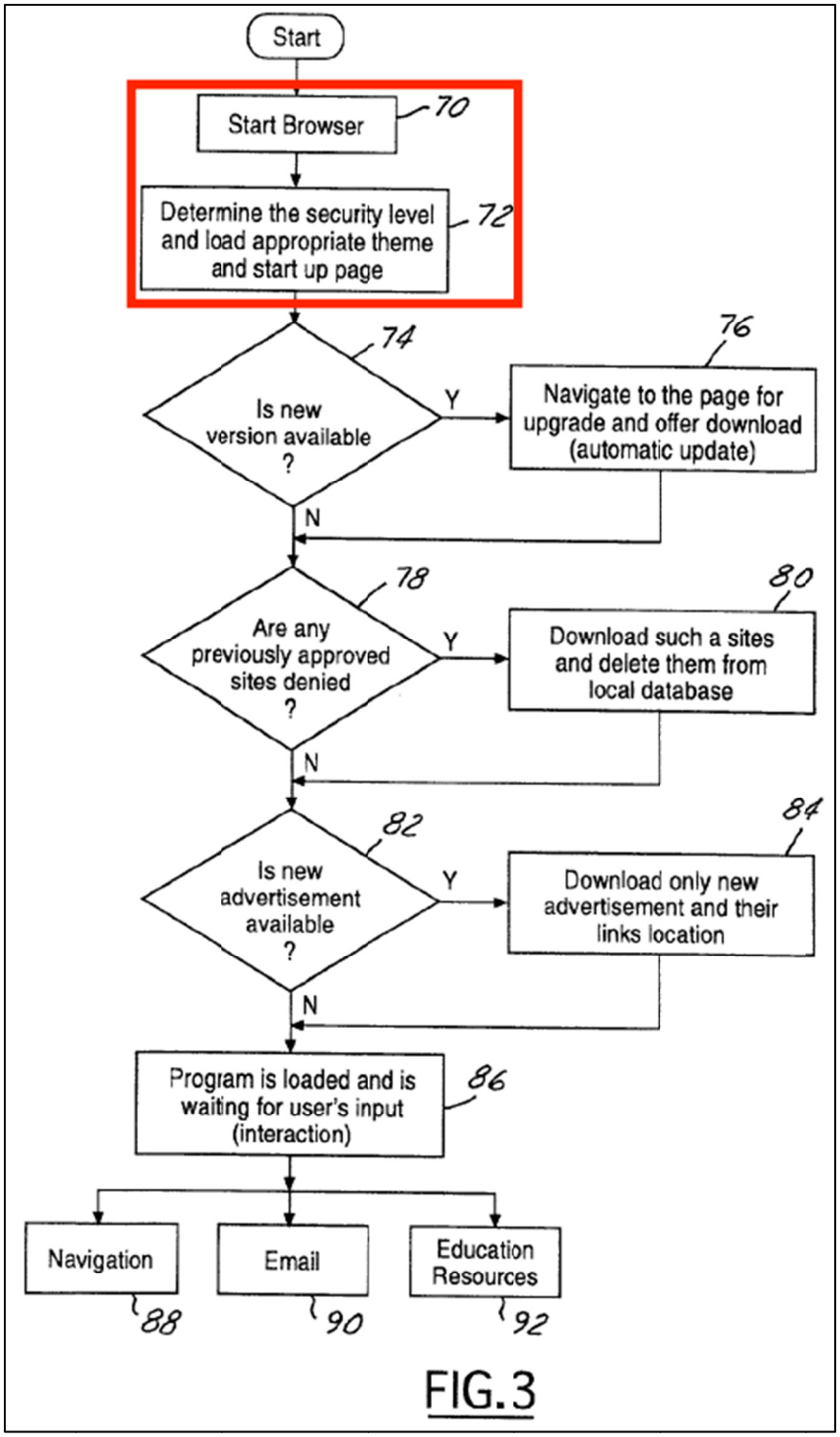


FIG.3

Spusta explains, with respect to Fig. 3:

[T]he browsing process is started at start browser step 70.… The

> browser may then have a sign in or selection for the user's name which then determines the security level and load an appropriate theme in start up page for that user in step 72. In step 72, various start up pages may also be associated with various age levels. For example, grades 2 and under may have a first page, grades 3 through 7 a second page, and grades 8 through 12 a third page.

(EX1005, ¶[0058]). A POSA would have understood that the start-up page is a network site because it is displayed in the web browser (i.e., the claimed network browser software), which includes buttons that control the operation and navigation through the Internet. (EX1005, ¶[0055]).

Additionally, a POSA would have understood that because the start-up page is determined by the security level, it is not a fixed page, but a page determined by the database entries. Moreover, even if the startup pages were not interpreted as being a "network site" because they are not explicitly described as being websites requiring remote access, a POSA would have been motivated to implement startup pages as websites because it would have been a very efficient implementation in that only one webserver needs to handle a particular startup page rather than having it stored locally and such an implementation would have yielded predictable results. (EX1003, ¶156).

p. Claim 13[preamble]: The system of claim 1, wherein,"

See supra Sections IX(C)(1)(a)-(i).

q. Claim 13[a]: "the controller instructions are configured to enable each of the gateway units to customize and transmit advertising received via the second network interface to a user display coupled with the gateway, the advertising being customized in accordance with information received via at least one of the second network interface and the user interface."

In annotated Fig. 3 below, *Spusta* discloses that instructions from the controller (central controller 16) are configured to enable each of the local computers (i.e., the claimed "gateway units") to customize and transmit advertising received in the manner as claimed. (EX1003, ¶165).

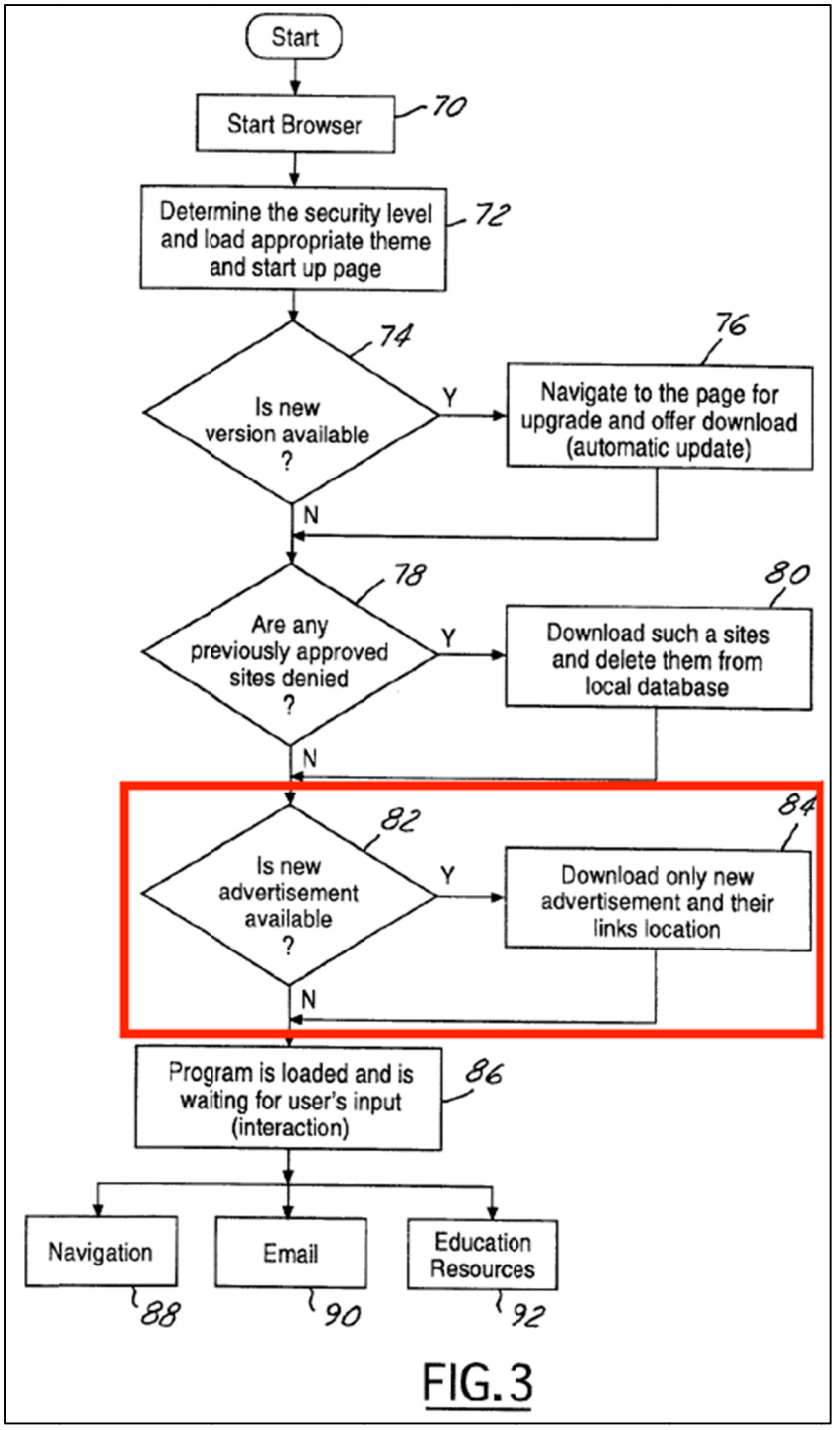


FIG. 3

In annotated Fig. 2 below, *Spusta* discloses that the advertising 50 will be shown on browser 38 of the user display. (EX1005, ¶[0057]; EX1003, ¶166).

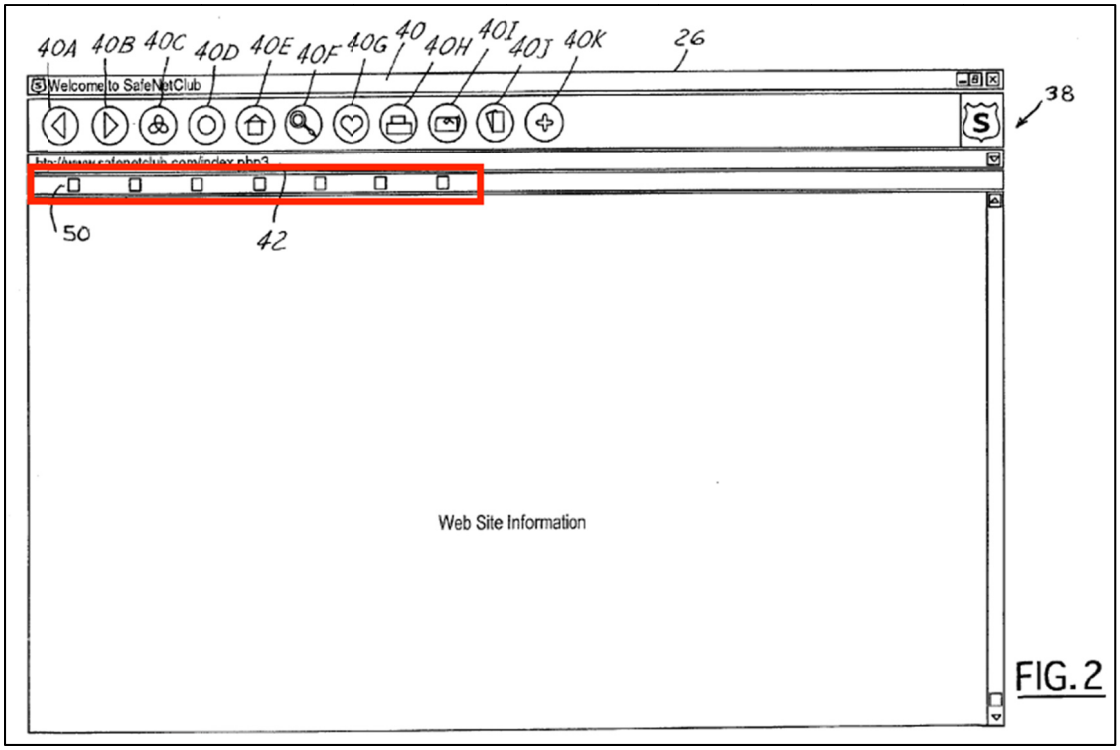


FIG. 2

Additionally, *Spusta* explains that the advertisements are customized via controller instructions received from the central controller and information received via the network interface:

> In step 82, advertising or sponsorship information may be provided to the screen display. In step 82, if new advertising is available, then step 84 is executed in which new advertising is loaded with their respective links onto the browser from the central computer.

(EX1005, ¶¶[0060], [0084]).

> Referring now to FIG. 10, the sponsorship/advertising method is illustrated. The method is started in block 210. **When this portion of the browser is invoked the advertising images or sponsorship images are obtained in step 212.** After steps 212 an ad code is sent and compared to ad code in 216. As illustrated in FIG. 11, **local**

> **computer may have a local computer ad code 200 while central computer may have a central computer ad code 202. Either the central computer ad code 202 may send its ad code to local computer for comparison step 216** or local computer may send its current ad code 200 to central computer 16. **Preferably, local computer 12 obtains central computer ad code 202 and compares the ad code therein.** As described above, each ad code preferably has bits corresponding to each of the ads that together form a digital word. If the ad code word 202 is different than the current local computer ad code 200, **the local computer 12 requests central computer 16 to update ad code 200 and the ads therein in step 218**.

(EX1005, ¶[0089], emphasis added).

Spusta further discloses that the advertisements are customized in accordance with information received via the user interface:

> In step 220 the user clicks on the specific subject button and a screen with the corresponding subject ad will be displayed in a window 26 as is best shown in FIG. 8. The ad display and window is performed in step 222. In this embodiment, a question is obtained from central computer 16 and provided on the display of the computer in step 224.

(EX1005, ¶[0089]). *See also* EX1003, ¶¶167-170.

r. Claim 23[preamble]: "A method for regulating access to a service provider network, the method comprising:"

See supra Section IX(B)(1)(a).

s. Claim 23[a]: "generating, by a controller node coupled to the service provider network, controller instructions,"

See supra Sections IX(B)(1)(b)-(c).

t. Claim 23[b]: "transmitting the controller instructions, by the controller node, to a plurality of gateway units of the service provider network,"

See supra Sections IX(B)(1)(d)-(e).

u. Claim 23[c]: "receiving, by the gateway units, user-entered content requests for the service provider network,"

See supra Sections IX(B)(1)(e)-(f).

v. Claim 23[d]: "receiving, by the gateway units, from the controller node, the controller instructions,"

See supra Section IX(B)(1)(g).

w. Claim 23[e]: "selectively transmitting, by the plurality of gateway units, the content requests to the service provider network in accordance with the controller instructions; and transferring, by the gateway units, received content data responsive to the transmitted content requests from the service provider network."

See supra Sections IX(B)(1)(h)-(i).

x. Claim 24[preamble]: "The method of claim 23"

See supra Sections IX(B)(1)(r)-(w).

y. Claim 24[a]: "further comprising storing the controller instructions, by the gateway units, in storage devices of the gateway units,"

See supra Section IX(B)(1)(k).

z. Claim 24[b]: "wherein each of the gateway units has an identifier that uniquely identifies the gateway unit."

See supra Section IX(B)(1)(l).

aa. Claim 32: "The method of claim 23, wherein the controller instructions include a pre-determined network site, and the method further comprises a gateway unit accessing the predetermined network site upon initiation of network browser software on the gateway unit, in accordance with the controller instructions."

See supra Section IX(B)(1)(o).

bb. Claim 34: "The method of claim 23, further comprising a gateway unit customizing and transmitting advertising received to a user display."

See supra Sections IX(B)(1)(p)-(w).

X. CONCLUSION

Petitioner respectfully requests that the PTAB institute an *inter partes* review and then proceed to cancel the challenged claims.

Respectfully submitted,

OBLON LLP

Dated: August 11, 2017

/Scott A. McKeown/
Scott A. McKeown
Reg. No. 42,866

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), the undersigned certifies that the foregoing document, excluding the portions exempted under 37 C.F.R. §42.24(a)(1), contains 13,689 words, including the words added in annotating the figures, which is under the limit of 14,000 words set by 37 C.F.R. §42.24(a)(1)(i).

Dated: August 11, 2017 By: /Scott A. McKeown/
Scott A. McKeown
Reg. No. 42,866

CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§42.6(e) and 42.105(b) on the Patent Owner by UPS Overnight Delivery of a copy of this Petition for *Inter Partes* Review and supporting materials at the correspondence address of record for the '468 Patent as well as counsel of record in the district court litigations:

Schwabe, Williamson & Wyatt, P.C.
1420 Fifth Avenue, Suite 3400
Seattle, WA 98101-4010

Isaac Phillip Rabicoff
Rabicoff Law
73 W Monroe St
Chicago, Illinois 60603

Dated: August 11, 2017 By: /Scott A. McKeown/
Scott A. McKeown
Reg. No. 42,866