



- (51) International Patent Classification:  
H04L 29/12 (2006.01)
- (21) International Application Number:  
PCT/US2016/061679
- (22) International Filing Date:  
11 November 2016 (11.11.2016)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
62/254,308 12 November 2015 (12.11.2015) US  
15/348,905 10 November 2016 (10.11.2016) US
- (71) Applicant: VERISIGN, INC. [US/US]; 12061 Bluemont Way, Reston, Virginia 20190 (US).
- (72) Inventor: THAKAR, Sameer; 12061 Bluemont Way, Reston, Virginia 20190 (US).
- (74) Agents: CAREY, John C. et al.; ARTEGIS LAW GROUP, LLP, 7710 Cherry Park Drive, Suite T104, Houston, Texas 77095 (US).

- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: TECHNIQUES FOR DIRECTING A DOMAIN NAME SERVICE (DNS) RESOLUTION PROCESS

(57) Abstract: In one embodiment, a privacy and security engine enables a user to specify a recursive resolver for a domain name service (DNS) resolution process. The privacy and security engine receives default DNS settings that specify a default recursive resolver to be implemented as a recursive resolver for the DNS resolution process. The default DNS settings are provided by an underlying mobile operator network to which the user device is connected. The privacy and security engine causes the user device to disregard the default DNS settings and implement customized DNS settings that specify a preferred recursive resolver to be implemented as the recursive resolver for the DNS resolution process. The customized DNS settings are associated with an activated privacy and security mode. Unlike conventional approaches to overriding DNS settings, the user is able to specify the recursive resolver that implements the DNS resolution process irrespective of the underlying network.

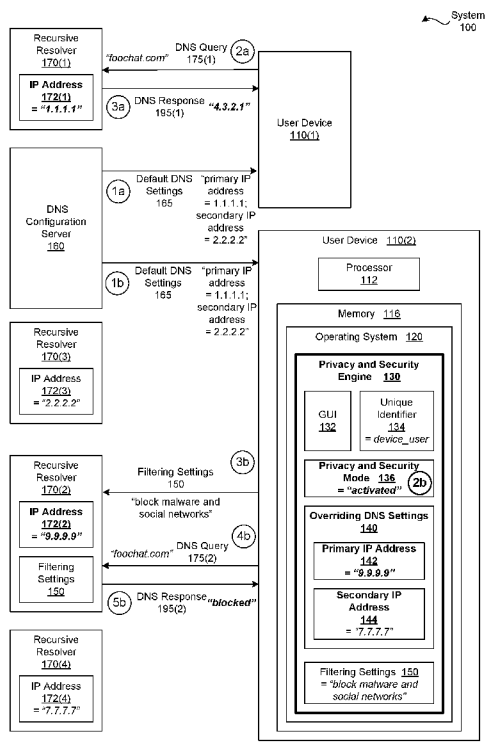


FIGURE 1

WO 2017/083759 A1

**Published:**

— *with international search report (Art. 21(3))*

## TECHNIQUES FOR DIRECTING A DOMAIN NAME SERVICE (DNS) RESOLUTION PROCESS

### CROSS-REFERENCE TO RELATED APPLICATIONS

5 [0001] This application claims the priority benefit of the U.S. patent application having  
Serial Number 15/348,905 (Attorney Docket Number SIGN/0048US) and filed on  
November 10, 2016, and U.S. provisional patent application having Serial Number  
62/254,308 (Attorney Docket Number 11569.0283-PRO) and filed on November 12,  
2015. The subject matter of these related applications is hereby incorporated herein  
10 by reference.

### BACKGROUND OF THE INVENTION

#### **Field of the Invention**

[0002] Embodiments of the present invention relate generally to computer networks  
and, more specifically, to techniques for directing a domain name service (DNS)  
15 resolution process.

#### **Description of the Related Art**

[0003] As is well-known, the domain name service (DNS) is the part of the Internet  
infrastructure that translates human-readable domain names into the Internet Protocol  
(IP) addresses needed to establish TCP/IP (Transmission Control Protocol/Internet  
20 Protocol) communication over the Internet. The DNS is the mechanism that allows  
users to refer to web sites and other Internet resources via intuitive domain names,  
such as "example.com," rather than the actual numeric IP addresses, e.g.,  
192.0.2.78, that are associated with different websites and other Internet resources.  
As referred to herein, an "Internet resource" may be any type of device or service that  
25 is accessible via the Internet.

[0004] Each domain name is typically made up of a series of character strings or  
"labels," where every two such character strings within the domain name are  
separated by a period. The right-to-left order of the labels within a domain name  
corresponds to a top-to-bottom order of domain names in a DNS hierarchy. To  
30 translate a particular domain name to a corresponding IP address, a DNS server,  
known as a "recursive resolver," traverses the DNS hierarchy in a process referred to  
herein as a "DNS resolution process."

[0005] To enable a user device to instigate the DNS resolution process, when the user device connects to an underlying network, the underlying network provides DNS settings that specify the recursive resolver for the DNS resolution process. However, the efficiency of the DNS resolution process, the operations performed during the DNS resolution process, and the resulting DNS responses may vary based on the specified recursive resolver. In particular, different recursive resolvers may implement different security functionality. For example, one recursive resolver could implement malware filtering and, consequently, would block access to a “malware” website. By contrast, another recursive resolver could lack malware filtering and, consequently, would allow access to the malware website. Further, the providers of different recursive resolvers may implement different privacy policies. For example, the provider of one recursive resolver could sell the contents of DNS queries to multiple external companies, while the provider of another recursive resolver could treat DNS queries as confidential.

[0006] To enable a user to direct the DNS resolution process to reflect user preferences, such as preferences regarding performance, privacy, security, and the like, some user devices implement “DNS controls.” In general, DNS controls allow a user to override the DNS settings provided by certain underlying networks with DNS settings that specify the recursive resolver for the DNS process as a preferred recursive resolver. DNS controls typically enable a user to override the DNS settings provided by enterprise networks, Internet Service Provider (ISP) networks, and Wi-Fi networks. However, DNS controls are unable to override the DNS settings provided by mobile operator networks, such as a Verizon network and a Sprint network. Accordingly, while a user device is connected to a mobile operator network, the DNS resolution process is performed by the recursive resolver selected by the mobile operator instead of the recursive resolver selected by the user.

[0007] As the foregoing illustrates, what is needed in the art are more effective techniques for specifying the recursive resolver for the domain name service resolution process.

## **SUMMARY OF THE INVENTION**

[0008] One embodiment of the present invention sets forth a method for specifying a recursive resolver for a domain name service (DNS) resolution process. The method includes receiving a first set of DNS settings that is associated with an underlying

mobile operator network to which a user device is connected, where the first set of DNS settings specifies a first recursive resolver to be implemented as a recursive resolver for a DNS resolution process; and causing the user device to disregard the first set of DNS settings and implement a second set of DNS settings that is

5 associated with an activated privacy and security mode, where the second set of DNS settings specifies a second recursive resolver to be implemented as the recursive resolver for the DNS resolution process.

[0009] Further embodiments provide, among other things, a computer-readable medium and a system configured to implement the method set forth above.

10 [00010] One advantage of the disclosed techniques is that a user may specify a preferred recursive resolver irrespective of the underlying network to which the user device is connected. The preferred recursive resolver may reflect user preferences, such as preferences regarding performance, privacy, security, and the like. By contrast, conventional DNS controls for specifying a preferred recursive resolver are  
15 unable to override the DNS settings provided by mobile operator networks.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

[0010] So that the manner in which the above recited features of the present invention can be understood in detail, a more particular description of the invention, briefly summarized above, may be had by reference to embodiments, some of which are  
20 illustrated in the appended drawings. It is to be noted, however, that the appended drawings illustrate only typical embodiments of this invention and are therefore not to be considered limiting of its scope, for the invention may admit to other equally effective embodiments.

[0011] Figure 1 is a conceptual illustration of a system configured to implement one or  
25 more aspects of the present invention;

[0012] Figure 2 illustrates an example of the graphical user interface of Figure 1, according to various embodiments of the present invention; and

[0013] Figure 3 is a flow diagram of method steps for selecting a recursive resolver for a domain name service (DNS) resolution process, according to various embodiments  
30 of the present invention.

## **DETAILED DESCRIPTION**

[0014] In the following description, numerous specific details are set forth to provide a more thorough understanding of the present invention. However, it will be apparent to one of skilled in the art that the present invention may be practiced without one or  
5 more of these specific details.

### **System Overview**

[0015] Figure 1 is a conceptual illustration of a system 100 configured to implement one or more aspects of the present invention. As shown, the system 100 includes, without limitation, user devices 110, recursive resolvers 170, and a domain name  
10 system (DNS) configuration server 160. In alternate embodiments, the system 100 may include any number of user devices 110, any number of recursive resolvers 170, and any number of DNS configuration servers 160, in any combination. For explanatory purposes, multiple instances of like objects are denoted with reference numbers identifying the object and parenthetical numbers identifying the instance  
15 where needed.

[0016] Each of the user devices 110 may be any type of device that is capable of communicating with other devices. For example, the user devices 110 could include conventional computing devices, smart phones, wearable technology devices, appliances (e.g. washer/dryers that utilize network communications, smart thermostat  
20 systems, etc.), sensors (e.g. remote monitoring heart monitoring implants, biochip transponders, automobiles sensors, etc.), traffic lights, parking meters, and the like.

[0017] As shown for the user device 110(2), the user devices 110 include, without limitation, a processor 112 and a memory 116. The processor 112 may be any instruction execution system, apparatus, or device capable of executing instructions.  
25 For example, the processor 112 could comprise a central processing unit (CPU), a digital signal processor (DSP), a controller, a microcontroller, a state machine, or any combination thereof.

[0018] The memory 116 stores content, such as software applications and data, for use by the associated processor 112. The memory 116 may be any type of non-  
30 volatile memory capable of storing data and software applications, such as a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash ROM), or any suitable combination of the foregoing.

In some embodiments, a storage (not shown) may supplement or replace the memory 116. The storage may include any number and type of external memories that are accessible to the processor 112. For example, and without limitation, the storage may include a Secure Digital Card, an external Flash memory, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing.

[0019] As shown, the memory 116 includes, without limitation, an operating system (OS) 120. The OS 120 is a software application that supports fundamental functions of the user device 110. Examples of fundamental functions include scheduling tasks, executing other software applications, managing hardware and software resources including the memory 116, controlling peripheral devices (e.g., printers), and so forth. The OS 120 is capable of executing in highly privileged modes that enable the OS 120 to perform actions that other software applications are typically unable to perform. For example, oftentimes the OS 120 is capable of modifying system files that other software applications are not authorized to modify.

[0020] In alternate embodiments, each of the user devices 110, the recursive resolvers 170, and the DNS configuration server 160 may include any number (including zero) and types of processors 112 and any number (including zero) and types of memories 116 in any combination. The processor 112 and the memory 116 may be implemented in any technically feasible fashion. For example, and without limitation, in various embodiments, the processor 112 and/or the memory 116 may be implemented as a stand-alone chip or as part of a more comprehensive solution that is implemented as an application-specific integrated circuit (ASIC) or a system-on-a-chip (SoC). In some embodiments, the user devices 110, the recursive resolvers 170, and the DNS configuration server 160 may interact with one or more clouds (e.g., encapsulated shared resources, software, data, etc.) to perform operations associated with the system 100. In such embodiments, the processor 112 and/or the memory 116 may be implemented in the cloud instead of in the user devices 110, the recursive resolvers 170, and the DNS configuration server 160.

[0021] As a general matter, the system 100 includes, without limitation, entities and software that provide underlying technologies to support essential Internet functions, such as communications and security. In particular, the recursive resolvers 170 provide a portion of a framework that implements the domain name system (DNS)

protocol. For explanatory purposes, entities that provide the framework that implements the DNS protocol, including the recursive resolvers 170, are referred to herein as “DNS servers.” In alternate embodiments, the system 100 may include any number and types of other DNS servers in addition to the recursive resolvers 170.

5 For example, in various embodiments, the system 100 may include authoritative name servers and forwarding resolvers.

**[0022]** The DNS is the part of the Internet infrastructure that translates human-readable domain names into the Internet Protocol (IP) addresses 172 needed to establish TCP/IP (Transmission Control Protocol/Internet Protocol) communication  
10 over the Internet. The DNS is the mechanism that allows users to refer to web sites and other Internet resources via intuitive domain names, such as “example.com,” rather than the actual IP addresses 172, e.g., 192.0.2.78, that are associated with different websites and other Internet resources. As referred to herein, an “Internet resource” may be any type of device or service that is accessible via the Internet.

15 **[0023]** Each domain name is typically made up of a series of character strings or “labels,” where every two such character strings within the domain name are separated by a period. The right-to-left order of the labels within a domain name correspond to the top-to-bottom order of domain names in a DNS hierarchy. The right-most label in a domain name is known as the top-level domain (“TLD”).  
20 Examples of well-known TLDs are “com”; “net”; “org”; and the like. Each TLD supports second-level domains, listed immediately to the left of the TLD, e.g., the “example” level in “example.com”. Domains can nest within the hierarchy for many levels. To translate a given domain name to a corresponding IP address, the recursive resolver 170 traverses the DNS hierarchy. The process of traversing the  
25 DNS hierarchy is referred to herein as a “DNS resolution process.”

**[0024]** In general, the DNS enables users to associate a variety of information with domain names based on resource records. For example, in addition to storing address records that map domain names to the corresponding IP addresses 172, the DNS stores service records (SRV) that identify services. Further, the DNS stores text  
30 records (TXT) that include arbitrary text and enable the DNS to serve as a general purpose database. A hierarchy of the DNS servers included in the system 100 maintain the resource records in large databases.



[0025] In operation, to enable the user device 110 to access information that is associated with a domain name, when the user device 110 connects to an underlying network, a DNS configuration server 160 that is associated with the underlying network provides default DNS settings 165. The underlying network comprises any number and type of physical links (e.g., wireless, wired, etc.) that connect the user device 110 to the Internet. Examples of underlying networks include mobile operator networks (e.g., Verizon) enterprise networks, Internet Service Provider (ISP) networks, Wi-Fi networks, and the like.

[0026] The DNS configuration server 160 may be any server that provides configuration information for the underlying network. For instance, in some embodiments, the DNS configuration server 160 comprises a Dynamic Host Configuration Protocol (DHCP) server. In addition to providing the default DNS settings 165, the DHCP server manages a pool of the IP addresses 172 and assigns the IP addresses 172 to entities (including the user devices 110) on the underlying network on-demand.

[0027] The default DNS settings 165 include, without limitation, the IP addresses 172 of both a “primary” recursive resolver 170(1) and a “secondary” recursive resolver 170(3). In a “default DNS resolution process,” the default DNS settings 165 specify the recursive resolver 170 that executes the DNS resolution process for the user device 110. The recursive resolver 170 that executes the DNS resolution process is referred to herein as “the recursive resolver 170 for the DNS resolution process.”

[0028] To access information that is associated with a domain name, the user device 110 generates a DNS query 175 that specifies the domain name. The user device 110 then attempts to transmit the DNS query 175 to the primary recursive resolver 170(1) specified in the default DNS settings 195. In response to the DNS query 175, the primary recursive resolver 170(1) executes the DNS resolution process to generate a DNS response 195 to the DNS query 175. If the primary recursive resolver 170(1) is unavailable (e.g., due to a power outage), then the user device 110 transmits the DNS query 175 to the secondary recursive resolver 170(3) specified in the default DNS settings 195. In response to the DNS query 175, the secondary recursive resolver 170(3) executes the DNS resolution process to generate the DNS response 195 to the DNS query 175.

[0029] The user device 110 may generate and transmit the DNS query 175 to the recursive resolver 170 in any technically feasible fashion. In some embodiments, the OS 120 may generate and transmit the DNS query 175 to the recursive resolver 170. In alternate embodiments, the user device 110 may include a stub resolver that generates and transmits the DNS query 175 to the recursive resolver 170. The user device 110 may generate and transmit the DNS query 175 to the recursive resolver 170 in response to any type of event. For example, suppose that a user visits a website “example.com” via a web browser executing on the user device 110. Further, suppose that a cache associated with the OS 120 executing on the user device 110 does not include a suitable translation for “example.com” to the corresponding IP address 172. In such a scenario, the OS 120 could generate and transmit the DNS query 175 (requesting the IP address 172 associated with “example.com”) to the recursive resolver 170.

[0030] For explanatory purposes only, Figure 1 depicts a sequence of events involved in a default DNS resolution process using a series of bubbles labeled 1a, 2a, and 3a. First, as depicted with the bubble labeled 1a, the user device 110(1) receives the default DNS settings 165 from the DNS configuration server 160. As shown, the default DNS settings 165 includes the primary IP address 172 of “1.1.1.1” associated with the recursive resolver 170(1). As depicted with the bubble labeled 2a, the user device 110(2) then transmits the DNS query 175(1) to the recursive resolver 170(1). The DNS query 175(1) requests the IP address 172 of the website “foochat.com.” In response, as depicted with the bubble labeled 3a, the recursive resolver 170(1) transmits the DNS response 195(1) to the user device 110(1). The DNS response 195(1) specifies the IP address 172 “4.3.2.1.”

[0031] As persons skilled in the art will recognize, the efficiency of the DNS resolution process, the operations performed during the DNS resolution process, and the resulting DNS responses 175 may vary based on the recursive resolver 170. For instance, oftentimes different recursive resolvers 170 implement different privacy and security functionality. Notably, the recursive resolver 170(1) that generates the DNS response 195(1) as part of the default DNS resolution process does not implement any privacy or security functionality. By contrast, the recursive resolver 170(2) implements a variety of techniques to preserve the privacy of the DNS queries 175 and enforce filter settings 150. The filtering settings 150 are typically configurable

settings that specify whether an access to a particular website, types of website, particular information, or types of information is authorized.

[0032] To enable a user to direct the DNS resolution process to reflect user preferences, such as preferences regarding performance, privacy, security, and the like, some user devices 110 implement “DNS controls.” In general, DNS controls allow a user to override the default DNS settings 165 provided by certain underlying networks with DNS settings that specify that a “preferred” recursive resolver 175 that is to be implemented as the recursive resolver 170 for the DNS process. The “preferred” recursive resolver 170 reflects the user preferences.

[0033] Conventional DNS controls typically enable a user to override the default DNS settings 165 provided by enterprise networks, Internet Service Provider (ISP) networks, and Wi-Fi networks. However, conventional DNS controls are unable to override the default DNS settings 165 provided by mobile operator networks, such as a Verizon network and a Sprint network. Accordingly, while a user device 110 is connected to a mobile operator network, the DNS resolution process is performed by the recursive resolver 170 selected by the mobile operator instead of the recursive resolver 170 selected by the user.

### **Enabling Comprehensive User Directed DNS Resolution**

[0034] To enable the user to direct the DNS resolution process to reflect user preferences in a more comprehensive fashion, the OS 120 includes, without limitation, a privacy and security engine 130. The privacy and security engine 130 comprises a software program that generally resides with the memory 116 and is executed by the processor 112 associated with the user device 110. As persons skilled in the art will recognize, because the privacy and security engine 130 is part of the OS 120, the privacy and security engine 130 may perform operations (e.g., access system files, etc) that conventional DNS controls are unable to implement. In particular, the privacy and security engine 130 is capable of overriding the default DNS settings 165 provided by any underlying network, including a mobile operator network.

[0035] The privacy and security engine 130 may cause the user device 110 to override the default DNS settings 165 in any technically feasible fashion. For instance, in some embodiments, the privacy and security engine 130 may cause the

user device 110 to disregard the default DNS settings 165 and implement overriding DNS settings 140 that are associated with a privacy and security mode 136. More specifically, in some embodiments the privacy and security engine 130 may overwrite the IP address 172 that is stored in a protected memory location that identifies the primary recursive resolver 170. In addition, the privacy and security engine 130 may overwrite the IP address 172 that is stored in a protected memory location that identifies the secondary recursive resolver 170.

**[0036]** In alternate embodiments, the privacy and security engine 130 may be implemented in any technically feasible fashion that enables the privacy and security engine 130 to override the default DNS settings 165 irrespective of the underlying network that provides the default DNS settings 165. In various embodiments, the functionality of the privacy and security engine 130 is integrated into or distributed across any number (including one) of software applications. For instance, in various embodiments, the privacy and security engine 130 may be implemented as a software application that is not included in the OS 120 and may or may not interact with the OS 120. In other embodiments, a portion or all of the functionality of the privacy and security engine 130 may be integrated into a stub resolver.

**[0037]** The privacy and security engine 130 described herein is not limited to any particular system 100 and may be adapted to take advantage of new systems 100 as they become available. In alternate embodiments, the functionality of the privacy and security engine 130 may be implemented and provided in any technically feasible. For instance, in some embodiments the privacy and security engine 130 may be provided as an application program (or programs) stored on computer readable media such as a CD-ROM, DVD-ROM, flash memory module, or other tangible storage media.

**[0038]** As shown, the privacy and security engine 130 includes, without limitation, a graphical user interface (GUI) 132, a unique identifier 134, the privacy and security mode 136, the overriding DNS settings 140 and the filtering settings 150. In operation, the privacy and security engine 130 displays the GUI 132 as part of a system-level GUI (not shown in Figure 1) that is provided by the user device 110. In general, the GUI 132 enables the user to specify user preferences that are associated with selecting and/or configuring the recursive resolver 170 for the DNS resolution process. In alternate embodiments, the GUI 132 may be replaced with any user

interface that enables the user to specify any number and type of user preferences that are associated with the DNS resolution process.

**[0039]** The unique identifier 134 may be any type of identifier that is based on the device 110, the user, and/or any number of other distinguishing characteristics that may be associated with DNS queries 175, in any combination. The unique identifier 134 may be associated with the DNS queries 175 in any technically feasible fashion and at any level of granularity. In some embodiments, the unique identifier 134 comprises the IP address 172 associated with the user device 110. In other embodiments, the unique identifier 134 is based on both the IP address 172 associated with the user device 110 and a user identification. For example, the unique identifier 134 could be a combination of the IP address 172 associated with the user device 110 and a user name.

**[0040]** In yet other embodiments, the unique identifier 134 may identify an organization within a company. Accordingly, the unique identifier 134 for a given user device 110 may match the unique identifier 134 for other user devices 110. In various embodiments, the device 110 may include multiple instances of the privacy and security engine 130, and different instances may include different unique identifiers 134, different privacy and security modes 136, different overriding DNS settings 140, and/or different filtering settings 150.

**[0041]** The privacy and security mode 136 may be either “deactivated” or “activated.” If the privacy and security mode 136 is deactivated, then the privacy and security engine 130 does not alter the default DNS resolution process. More precisely, the privacy and security engine 130 does not override the default DNS settings 165 provided by the underlying network. By contrast, if the privacy and security mode 136 is “activated,” then the privacy and security engine 130 overrides the default DNS settings 165 with the overriding DNS settings 140.

**[0042]** As shown, the overriding DNS settings 140 include, without limitation, a primary IP address 142 and a secondary IP address 144. The primary IP address 142 specifies the IP address 172 associated with a user-selected primary recursive resolver 170 and the secondary IP address 142 specifies the IP address 172 associated with a user-selected secondary recursive resolver 170. In general, the

user sets the overriding DNS settings 140 via the GUI 132 to specify a pair of recursive resolvers 170 that comply with the user preferences.

[0043] If the privacy and security mode 136 is activated, then to obtain information that is associated with a domain name, the user device 110 implements a “user directed DNS resolution process” instead of the default DNS resolution process. In the user directed DNS resolution process, the user device 110 generates the DNS query 175 that specifies the domain name. The user device 110 then attempts to transmit the DNS query 175 to the user-selected primary recursive resolver 170(2) specified by the primary IP address 142 included in the overriding DNS settings 140. In response to the DNS query 175, the user-selected primary recursive resolver 170(2) executes the DNS resolution process to generate a DNS response 195 to the DNS query 175.

[0044] If the user-selected primary recursive resolver 170(2) is unavailable (e.g., due to a power outage), then the user device 110 transmits the DNS query 175 to the user-selected secondary recursive resolver 170(4) specified by the secondary IP address 144 included in the overriding DNS settings 140. In response to the DNS query 175, the user-selected secondary recursive resolver 170(4) executes the DNS resolution process to generate the DNS response 195 to the DNS query 175.

[0045] In some embodiments, the privacy and security engine 130 implements a list of predetermined DNS settings. As part of prompting the user to specify the overriding DNS settings 140, the GUI 132 displays the list of predetermined DNS settings. The user may set the overriding DNS settings 140 equal to one of the predetermined DNS settings or explicitly enter the primary IP address 142 and the secondary IP address 144 included in the overriding DNS settings 140. In general, the privacy and security engine 130 and the GUI 132 may implement the predetermined DNS settings in any technically feasible fashion.

[0046] One of the predetermined DNS settings 140 is the default DNS setting 165. If the user sets the overriding DNS settings 140 equal to the default DNS setting 165, then the privacy and security engine 130 deactivates the privacy and security mode 136. Further, because the privacy and security engine 130 may have previously disregarded the default DNS setting 165 provided by the underlying network, the privacy and security engine 130 transmits a network poll to the DNS configuration

server 160 to request the default DNS settings 165. The privacy and security engine 130 then selects the recursive resolver 170 for the DNS resolution process based on the default DNS settings 165. In alternate embodiments, the privacy and security engine 130 may obtain the default DNS settings 165 in response to any type of event and in any technically feasible fashion.

**[0047]** The filtering settings 150 may include any number and type of configurable settings that are compatible with the recursive resolvers 170 specified in the overriding DNS settings 140. In operation, after the user selects the overriding DNS settings 140 via the GUI 132, the privacy and security engine 130 attempts to ascertain the capabilities of the recursive resolvers 170 specified in the overriding DNS settings 140. The privacy and security engine 130 may attempt to ascertain the capabilities of the recursive resolvers 170 in any technically feasible fashion.

**[0048]** For instance, for each of the predetermined DNS settings , the privacy and security engine 130 includes the filtering settings 150 that are supported by the corresponding recursive resolvers 170. If the user selects one of the predetermined DNS settings as the overriding DNS settings 140, then the privacy and security engine 130 configures the GUI 132 to display widgets (e.g., menus, radio buttons, etc.) that enable the user to select values for the supported filtering settings 150. The privacy and security engine 130 and the GUI 132 may implement the predetermined DNS settings 140 and store the associated filtering settings 150 in any technically feasible fashion.

**[0049]** The filtering settings 150 may include any number and type of settings that customize the DNS resolution operations performed by the recursive resolver 170. For example, the filtering settings 150 could include parental controls that enable a parent to block websites that are associated with malware, specified categories (e.g., gambling, social networks, videos, etc.), or a blacklist. In another example, the filtering settings 150 could include controls that configure the recursive resolver 170 to block access to all Internet resources that are not specified in a whitelist.

**[0050]** After the user selects the filtering settings 150 via the GUI 132, the privacy and security engine 130 causes the recursive resolvers 170 specified by the overriding DNS settings 140 to implement the filtering settings 150. The privacy and security engine 130 may perform any number of configuration operations in any technically

feasible fashion. For example, the privacy and security engine 130 could transmit the filtering settings 150 and the unique identifier 134 to the recursive resolver 150 to configure the recursive resolver 170 to apply the filtering settings 150 when processing DNS queries 175 that are associated with the unique identifier 134. In  
5 alternate embodiments, the privacy and security engine 130 may transmit any amount of information instead of or in addition to the unique identifier 134 to configure the recursive resolver 170 to apply the filtering settings 150.

**[0051]** In some embodiments, as part of enforcing the filtering settings 150, the privacy and security engine 130 may cause the user device 110 to transmit identifying  
10 information to the recursive resolver 150 in conjunction with the DNS queries 175. For example, in some embodiments, the privacy and security engine 130 may cause the user device 110 to attach the unique identifier 134 to DNS queries 175 in a manner that complies with a protocol that is implemented in the recursive resolver 170. In other embodiments, the recursive resolver 170 may obtain and/or derive the  
15 unique identifier 134 in any technically feasible fashion without receiving any additional information from the user device 110, the OS 120, or the privacy and security engine 130.

**[0052]** Advantageously, the privacy and security engine 130 maintains the user preferences specified via the GUI 132 irrespective of the underlying network. For  
20 example, suppose that the privacy and security mode 136 for a given user device 110 is activated when the user device 110 is connected to an ISP network. The privacy and security engine 130 ensures that the user device 110 transmits the DNS queries 175 to the recursive resolver 170 that is specified by the overriding DNS settings 140. Subsequently, suppose that user device 110 disconnects from the ISP network and  
25 connects to a mobile operator network. The DNS configuration server 160 associated with the mobile operator network transmits new default DNS settings 165 to the user device 110. However, the privacy and security engine 130 ensures that the user device 110 disregards the default DNS settings 165 and continues to transmits the DNS queries 175 to the recursive resolver 170 that is specified by the  
30 overriding DNS settings 140.

**[0053]** For explanatory purposes only, Figure 1 depicts a sequence of events involved in a user directed DNS resolution process using a series of bubbles labeled 1b-5b. Although not shown in Figure 1, the privacy and security mode 136 associated with



the user device 110(2) is initially deactivated. First, as depicted with the bubble labeled 1b, the user device 110(2) receives the default DNS settings 165 from the DNS configuration server 160. As shown, the default DNS settings 165 includes the primary IP address 172 “1.1.1.1” that is associated with the recursive resolver 170(1).

5 Since the privacy and security mode 136 is deactivated, the privacy and security engine 130 sets the recursive resolver 170 for the DNS resolution process equal to the recursive resolver 170(1).

[0054] Subsequently, as depicted with the bubble labeled 2b, the user activates the privacy and security mode 136 via the GUI 132. The overriding DNS settings 140 is  
10 one of the predetermined DNS settings, and includes the primary IP address 142 “9.9.9.9.” Accordingly, the privacy and security engine 130 disregards the default DNS settings 165 and set the recursive resolver 170 for the DNS resolution process equal to the recursive resolver 170(2) that is associated with the IP address 142 “9.9.9.9.” Further, as depicted with the bubbled labeled 3b, the privacy and security  
15 engine 130 transmits the user-configured filtering settings 150 “block malware and social networks” to the recursive resolver 170(2).

[0055] As depicted with the bubble labeled 4b, the user device 110(2) then transmit the DNS query 175(2) to the recursive resolver 170(2). The DNS query 175(2) requests the IP address 172 of the website “foochat.com.” In response, the recursive  
20 resolver 170(2) determines that the website “foochat.com” is associated with social networks. Consequently, as depicted with the bubble labeled 5b, the recursive resolver 170(2) transmits the DNS response 195(2) “blocked” to the user device 110(2), thereby enforcing the user preferences.

[0056] Figure 2 illustrates an example of the graphical user interface (GUI) 132 of  
25 Figure 1, according to various embodiments of the present invention. As shown, the GUI 132 is accessed via a “privacy and security” radio button that is included in a system-level GUI 210.

[0057] After the user activates the “privacy and security” radio button, the privacy and security engine 130 configures the GUI 132 to display a privacy and security menu  
30 220. The privacy and security menu 220 enables the user to access a DNS settings submenu 230 and a parental controls submenu 240. The DNS settings submenu 230 includes radio buttons that enable the user to set the overriding DNS settings 140

equal to predetermined DNS settings. The DNS settings submenu 230 also includes text entry fields that enable the user to explicitly specify the overriding DNS settings 140. As shown, the user sets the overriding DNS settings 140 equal to the predetermined DNS settings associated with "Verisign."

5 [0058] The parental controls submenu 240 enables the user to block websites that are associated with malware, access a category blocking submenu 250, specify a whitelist, and specify a blacklist. As shown, the user activates malware blocking and accesses the category blocking submenu 250. The category blocking submenu 250 includes a variety of categories. As shown, the user activates a "social networks"  
10 radio button that is included in the category blocking submenu 250 to block websites that are associated with social networks. In various embodiments, the privacy and security engine 130 may configure the GUI 132 to display any number and type of widgets that enable the user to specify the filtering settings 150. Further, the recursive resolver 170 may implement the filtering settings 150 in any technically  
15 feasible fashion. For example, if a whitelist is specified, then the recursive resolver 170 could be configured to override any of the other filtering settings 150 with the whitelist.

[0059] As a result of the depicted user selections, the privacy and security engine 130 sets the recursive resolver 120 for the DNS resolution process to the "Verisign"  
20 recursive resolver 170. Further, the privacy and security engine 130 configures the Verisign recursive resolver 170 to implement the filtering settings 150 "block malware and social network" for the DNS queries 175 that are associated with the unique identifier 134.

### Directing a DNS Resolution Process

25 [0060] Figure 3 is a flow diagram of method steps for selecting a recursive resolver for a domain name system (DNS) resolution process, according to various embodiments of the present invention. Although the method steps are described with reference to the systems of Figures 1-2, persons skilled in the art will understand that any system configured to implement the method steps, in any order, falls within the  
30 scope of the present invention.

[0061] As shown, a method 300 begins at step 306, where the privacy and security engine 130 included in a user device 120 receives input data associated with the DNS

resolution process. The input data may be configuration data from the GUI 132 included in the privacy and security engine 130 or the default DNS settings 165 from the DNS configuration server 160.

**[0062]** At step 308, the privacy and security engine 130 determines whether the privacy and security mode 136 is activated. If, at step 308, the privacy and security engine 130 determines that the privacy and security mode is not activated, then the method 300 proceeds to step 310. At step 310, the privacy and security engine 130 causes the user device 110 to select the recursive resolver 170 for the DNS resolution process based on the default DNS settings 165.

**[0063]** As part of step 310, the privacy and security engine 130 may request the default DNS settings 165 from the DNS configuration server 160 associated with the underlying network. For example, suppose that the configuration data indicates that the user deactivated the privacy and security mode 136. The privacy and security engine 130 would request the default DNS settings 165 from the DNS configuration server 160 associated with the underlying network. The method 300 then returns to step 306, where the privacy and security engine 130 receives and processes new input data.

**[0064]** If, however, at step 308, the privacy and security engine 130 determines that the privacy and security model 136 is activated, then the method 300 proceeds directly to step 312. At step 312, the privacy and security engine 130 causes the user device 110 to select the recursive resolver 170 for the DNS resolution process based on the overriding DNS settings 140. The privacy and security engine 130 may cause the user device 110 to select the recursive resolver 170 for the DNS resolution process in any technically feasible fashion. For instance, in some embodiments, the privacy and security engine 130 overwrites a protected memory location that stores the default DNS settings 165 with the overriding DNS settings 140.

**[0065]** At step 314, the privacy and security engine 130 determines whether the privacy and security engine 130 is capable of configuring the selected recursive resolver 170 to implement the filtering settings 150. If, at step 314, the privacy and security engine 130 determines that the privacy and security engine 130 is not capable of configuring the selected recursive resolver 170 to implement the filtering

settings 150, then the method 300 returns to step 306, where the privacy and security engine 130 receives and processes new input data.

**[0066]** If, however, at step 314, the privacy and security engine 130 determines that the privacy and security engine 130 is capable of configuring the selected recursive resolver 170 to implement the filtering settings 150, then the method 300 proceeds to  
5 step 316. At step 316, the privacy and security engine 130 configures the recursive resolver 170 to implement the filtering settings 150 for the DNS requests 175 that are associated with the unique identifier 134. The method 300 then returns to step 306, where the privacy and security engine 130 receives and processes new input data.

**[0067]** The privacy and security engine 130 may determine the unique identifier 134 and cause the recursive resolver 170 to implement the filtering settings 150 based on the unique identifier 134 in any technically feasible fashion. For instance, in some  
10 embodiments, the privacy and security engine 130 appends a user name to the IP address 172 associated with the user device 170 to generate the unique identifier 134. The privacy and security engine 130 then transmits the filtering settings 150 and  
15 the unique identifier 134 to the selected recursive resolver 170.

**[0068]** The privacy and security engine 130 continues to cycle through steps 306-316, receiving new input data and then selecting the recursive resolver 170 for the DNS resolution process based on the new input data. As the privacy and security engine  
20 130 executes, the user device 110 transmits the DNS queries 175 to the selected recursive resolver 170. In response, the user device 110 receives the DNS responses 195 from the selected recursive resolver 170. In some embodiments, the privacy and security engine 130 may cause the user device 110 to associate the unique identifier 134 with the DNS query 175 prior to transmitting the DNS query 175  
25 to the selected recursive resolver 170. In alternate embodiments, the privacy and security engine 130 or the user device 110 may cause the operating system 120 or any other software application to transmit the DNS queries 175 to the selected recursive resolver 170.

**[0069]** In sum, the disclosed techniques enable users to override the DNS settings  
30 provided by underlying networks. In operation, the operating system (OS) of the user device implements a privacy and security engine. The privacy and security engine includes a GUI that allows the user to activate a privacy and security mode, specify

overriding DNS settings, and specify filtering settings. When the user activates the privacy and security mode, the privacy and security engine selects the recursive resolver for the DNS resolution process based on the overriding DNS settings. The privacy and security engine then configures the selected recursive resolver to  
5 implement any specified filtering settings. Subsequently, the user device transmits DNS queries to the selected recursive resolver, disregarding the DNS settings provided by the underlying network.

**[0001]** Advantageously, the techniques described herein enable a user to select the recursive resolver for the DNS resolution process irrespective of the underlying  
10 network. Consequently, the user may select a recursive resolver that complies with user preferences (e.g., performance, privacy, security, etc.) during the DNS resolution process. By contrast, user devices that implement conventional DNS controls are unable to override the DNS settings provided by underlying mobile operator networks. As a result, the recursive resolver that implements the DNS resolution process when  
15 a user device that implements conventional DNS controls is connected to an underlying mobile operator network does not necessarily comply with the user preferences.

**[0070]** 1. In some embodiments a method for specifying a recursive resolver for a domain name service (DNS) resolution process comprises receiving a first set of DNS  
20 settings that is associated with an underlying mobile operator network to which a user device is connected, wherein the first set of DNS settings specifies a first recursive resolver to be implemented as a recursive resolver for a DNS resolution process; and causing the user device to disregard the first set of DNS settings and implement a second set of DNS settings that is associated with an activated privacy and security  
25 mode, wherein the second set of DNS settings specifies a second recursive resolver to be implemented as the recursive resolver for the DNS resolution process.

**[0071]** 2. The computer-implemented method of clause 1, further comprising receiving a third set of DNS settings that is associated with a new underlying network to which the user device is connected, wherein the third set of DNS settings specifies a third  
30 recursive resolver to be implemented as the recursive resolver for a DNS resolution process; and causing the user device to disregard the third set of DNS settings.

[0072] 3. The computer-implemented method of clauses 1 or 2, wherein the new underlying network comprises an enterprise network or an internet service provider (ISP) network.

[0073] 4. The computer-implemented method of any of clauses 1-3, further comprising, prior to causing the user device to disregard the first set of DNS settings receiving user input specifying one or more filtering settings that are associated with a first unique identifier corresponding to at least one of a user and the user device; and causing the second recursive resolver to implement the one or more filtering settings based on the first unique identifier.

[0074] 5. The computer-implemented method of any of clauses 1-4, wherein the one or more filtering settings comprise at least one of malware settings, category settings, a blacklist, and a whitelist.

[0075] 6. The computer-implemented method of any of clauses 1-5, further comprising causing the user device to associate the first unique identifier with a DNS query prior to transmitting the DNS query to the second recursive resolver.

[0076] 7. The computer-implemented method of any of clauses 1-6, wherein, in response to the DNS query, the second recursive resolver evaluates the DNS query based on the one or more filtering settings and the first unique identifier to determine that the DNS query is authorized; recursively traverses a DNS hierarchy to translate a domain name specified in the DNS query to a first Internet Protocol (IP) address that complies with the one or more filtering settings to generate a DNS response; and transmits the DNS response to the user device.

[0077] 8. The computer-implemented method of any of clauses 1-7, wherein, in response to the DNS query, the second recursive resolver evaluates the DNS query based on the one or more filtering settings and the first unique identifier to determine that the DNS query is not authorized; and blocks access to information requested in the DNS query.

[0078] 9. In some embodiments, a computer-readable storage medium includes instructions that, when executed by a processor, cause the processor to specify a recursive resolver for a domain name service (DNS) resolution process by performing the steps of receiving a first set of DNS settings that is associated with an underlying

mobile operator network to which a user device is connected, wherein the first set of DNS settings specifies a first recursive resolver to be implemented as a recursive resolver for a DNS resolution process; and causing the user device to disregard the first set of DNS settings and implement a second set of DNS settings that is  
5 associated with an activated privacy and security mode, wherein the second set of DNS settings specifies a second recursive resolver to be implemented as the recursive resolver for the DNS resolution process.

**[0079]** 10. The computer-readable storage medium of clause 9, further comprising receiving a third set of DNS settings that is associated with a new underlying network  
10 to which the user device is connected, wherein the third set of DNS settings specifies a third recursive resolver to be implemented as the recursive resolver for a DNS resolution process; and causing the user device to disregard the third set of DNS settings.

**[0080]** 11. The computer-readable storage medium of clause 9 or 10, wherein the  
15 new underlying network comprises an enterprise network or an internet service provider (ISP) network.

**[0081]** 12. The computer-readable storage medium of any of clauses 1-11, wherein the second set of DNS settings comprises a primary Internet Protocol (IP) address and a secondary IP address, and disregarding the first set of DNS settings and  
20 implementing the second set of DNS settings comprises selecting a server machine that is identified by the primary IP address or the secondary IP address as the recursive resolver for the DNS resolution process.

**[0082]** 13. The computer-readable storage medium of any of clauses 1-12, wherein disregarding the first set of DNS settings and implementing the second set of DNS  
25 settings comprises performing one or more write operations to store an IP address in a protected memory location that identifies the recursive resolver for the DNS resolution process, wherein the IP address is included in the second set of DNS settings and identifies the second recursive resolver.

**[0083]** 14. The computer-readable storage medium of any of clauses 1-13, further  
30 comprising, prior to causing the user device to disregard the first set of DNS settings receiving user input specifying one or more filtering settings that are associated with a

first unique identifier corresponding to at least one of a user and the user device; and causing the second recursive resolver to implement the one or more filtering settings based on the first unique identifier.

5 [0084] 15. The computer-readable storage medium of any of clauses 1-14, wherein the one or more filtering settings comprise at least one of malware settings, category settings, a blacklist, and a whitelist.

[0085] 16. The computer-readable storage medium of any of clauses 1-15, further comprising, prior to causing the user device to disregard the first set of DNS settings, activating the privacy and security mode based on user input.

10 [0086] 17. In some embodiments, a system comprises a memory storing a privacy and security engine; and a processor that is coupled to the memory and, when executing the privacy and security engine, is configured to receive a first set of domain name service (DNS) settings that is associated with an underlying mobile operator network to which a user device is connected, wherein the first set of DNS  
15 settings specifies a first recursive resolver to be implemented as a recursive resolver for a DNS resolution process; and cause the user device to disregard the first set of DNS settings and implement a second set of DNS settings that is associated with an activated privacy and security mode, wherein the second set of DNS settings specifies a second recursive resolver to be implemented as the recursive resolver for  
20 the DNS resolution process.

[0087] 18. The system of clause 17, wherein the privacy and security engine further configures the processor to receive a third set of DNS settings that is associated with a new underlying network to which the user device is connected, wherein the third set  
25 of DNS settings specifies a third recursive resolver to be implemented as the recursive resolver for a DNS resolution process; and cause the user device to disregard the third set of DNS settings.

[0088] 19. The system of clauses 18 or 19, wherein the new underlying network comprises an enterprise network or an internet service provider (ISP) network.

30 [0089] 20. The system of any of clauses 1-19, wherein the privacy and security engine further configures the processor to, prior to causing the user device to



disregard the first set of DNS settings, activate the privacy and security mode based on user input.

[0090] The descriptions of the various embodiments have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the 5 embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments.

[0091] Aspects of the present embodiments may be embodied as a system, method or computer program product. Accordingly, aspects of the present disclosure may 10 take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a “module” or “system.” Furthermore, aspects of the present disclosure may take the form of a computer program product embodied in one or more computer readable 15 medium(s) having computer readable program code embodied thereon.

[0092] Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, 20 infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only 25 memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, 30 or device.

[0093] Aspects of the present disclosure are described above with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and

computer program products according to embodiments of the disclosure. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program

5 instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, enable the implementation of the functions/acts specified in the flowchart and/or block diagram block or blocks. Such  
10 processors may be, without limitation, general purpose processors, special-purpose processors, application-specific processors, or field-programmable processors or gate arrays.

**[0094]** The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and  
15 computer program products according to various embodiments of the present disclosure. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the  
20 block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart  
25 illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

**[0095]** While the preceding is directed to embodiments of the present disclosure, other and further embodiments of the disclosure may be devised without departing  
30 from the basic scope thereof, and the scope thereof is determined by the claims that follow.

**WHAT IS CLAIMED IS:**

1. A computer-implemented method for specifying a recursive resolver for a domain name service (DNS) resolution process, the method comprising:

receiving a first set of DNS settings that is associated with an underlying

5 mobile operator network to which a user device is connected, wherein the first set of DNS settings specifies a first recursive resolver to be implemented as a recursive resolver for a DNS resolution process; and

causing the user device to disregard the first set of DNS settings and

10 implement a second set of DNS settings that is associated with an activated privacy and security mode, wherein the second set of DNS settings specifies a second recursive resolver to be implemented as the

recursive resolver for the DNS resolution process.

2. The computer-implemented method of claim 1, further comprising:

15 receiving a third set of DNS settings that is associated with a new underlying network to which the user device is connected, wherein the third set of DNS settings specifies a third recursive resolver to be implemented as the recursive resolver for a DNS resolution process; and

causing the user device to disregard the third set of DNS settings.

20

3. The computer-implemented method of claim 2, wherein the new underlying network comprises an enterprise network or an internet service provider (ISP) network.

25 4. The computer-implemented method of claim 1, further comprising, prior to causing the user device to disregard the first set of DNS settings:

receiving user input specifying one or more filtering settings that are associated with a first unique identifier corresponding to at least one of a user and the user device; and

30 causing the second recursive resolver to implement the one or more filtering settings based on the first unique identifier.

5. The computer-implemented method of claim 4, wherein the one or more filtering settings comprise at least one of malware settings, category settings, a blacklist, and a whitelist.

5 6. The computer-implemented method of claim 4, further comprising causing the user device to associate the first unique identifier with a DNS query prior to transmitting the DNS query to the second recursive resolver.

7. The computer-implemented method of claim 6, wherein, in response to the  
10 DNS query, the second recursive resolver:  
evaluates the DNS query based on the one or more filtering settings and the first unique identifier to determine that the DNS query is authorized;  
recursively traverses a DNS hierarchy to translate a domain name specified in the DNS query to a first Internet Protocol (IP) address that complies with  
15 the one or more filtering settings to generate a DNS response; and  
transmits the DNS response to the user device.

8. The computer-implemented method of claim 6, wherein, in response to the  
DNS query, the second recursive resolver:  
20 evaluates the DNS query based on the one or more filtering settings and the first unique identifier to determine that the DNS query is not authorized;  
and  
blocks access to information requested in the DNS query.

25 9. A computer-readable storage medium including instructions that, when executed by a processor, cause the processor to specify a recursive resolver for a domain name service (DNS) resolution process by performing the steps of:  
receiving a first set of DNS settings that is associated with an underlying mobile operator network to which a user device is connected, wherein  
30 the first set of DNS settings specifies a first recursive resolver to be implemented as a recursive resolver for a DNS resolution process; and  
causing the user device to disregard the first set of DNS settings and implement a second set of DNS settings that is associated with an activated privacy and security mode, wherein the second set of DNS

settings specifies a second recursive resolver to be implemented as the recursive resolver for the DNS resolution process.

10. The computer-readable storage medium of claim 9, further comprising:  
5 receiving a third set of DNS settings that is associated with a new underlying network to which the user device is connected, wherein the third set of DNS settings specifies a third recursive resolver to be implemented as the recursive resolver for a DNS resolution process; and  
causing the user device to disregard the third set of DNS settings.

10

11. The computer-readable storage medium of claim 10, wherein the new underlying network comprises an enterprise network or an internet service provider (ISP) network.

15

12. The computer-readable storage medium of claim 9, wherein the second set of DNS settings comprises a primary Internet Protocol (IP) address and a secondary IP address, and disregarding the first set of DNS settings and implementing the second set of DNS settings comprises selecting a server machine that is identified by the primary IP address or the secondary IP address as the recursive resolver for the DNS  
20 resolution process.

20

13. The computer-readable storage medium of claim 9, wherein disregarding the first set of DNS settings and implementing the second set of DNS settings comprises performing one or more write operations to store an IP address in a protected  
25 memory location that identifies the recursive resolver for the DNS resolution process, wherein the IP address is included in the second set of DNS settings and identifies the second recursive resolver.

25

14. The computer-readable storage medium of claim 9, further comprising, prior to  
30 causing the user device to disregard the first set of DNS settings:  
receiving user input specifying one or more filtering settings that are associated with a first unique identifier corresponding to at least one of a user and the user device; and

30

causing the second recursive resolver to implement the one or more filtering settings based on the first unique identifier.

15. The computer-readable storage medium of claim 14, wherein the one or more  
5 filtering settings comprise at least one of malware settings, category settings, a  
blacklist, and a whitelist.

16. The computer-readable storage medium of claim 9, further comprising, prior to  
causing the user device to disregard the first set of DNS settings, activating the  
10 privacy and security mode based on user input.

17. A system comprising:  
a memory storing a privacy and security engine; and  
a processor that is coupled to the memory and, when executing the privacy  
15 and security engine, is configured to:  
receive a first set of domain name service (DNS) settings that is  
associated with an underlying mobile operator network to which a  
user device is connected, wherein the first set of DNS settings  
specifies a first recursive resolver to be implemented as a  
20 recursive resolver for a DNS resolution process; and  
cause the user device to disregard the first set of DNS settings and  
implement a second set of DNS settings that is associated with  
an activated privacy and security mode, wherein the second set  
of DNS settings specifies a second recursive resolver to be  
25 implemented as the recursive resolver for the DNS resolution  
process.

18. The system of claim 17, wherein the privacy and security engine further  
configures the processor to:  
30 receive a third set of DNS settings that is associated with a new underlying  
network to which the user device is connected, wherein the third set of  
DNS settings specifies a third recursive resolver to be implemented as  
the recursive resolver for a DNS resolution process; and  
cause the user device to disregard the third set of DNS settings.

19. The system of claim 18, wherein the new underlying network comprises an enterprise network or an internet service provider (ISP) network.

- 5 20. The system of claim 17, wherein the privacy and security engine further configures the processor to, prior to causing the user device to disregard the first set of DNS settings, activate the privacy and security mode based on user input.

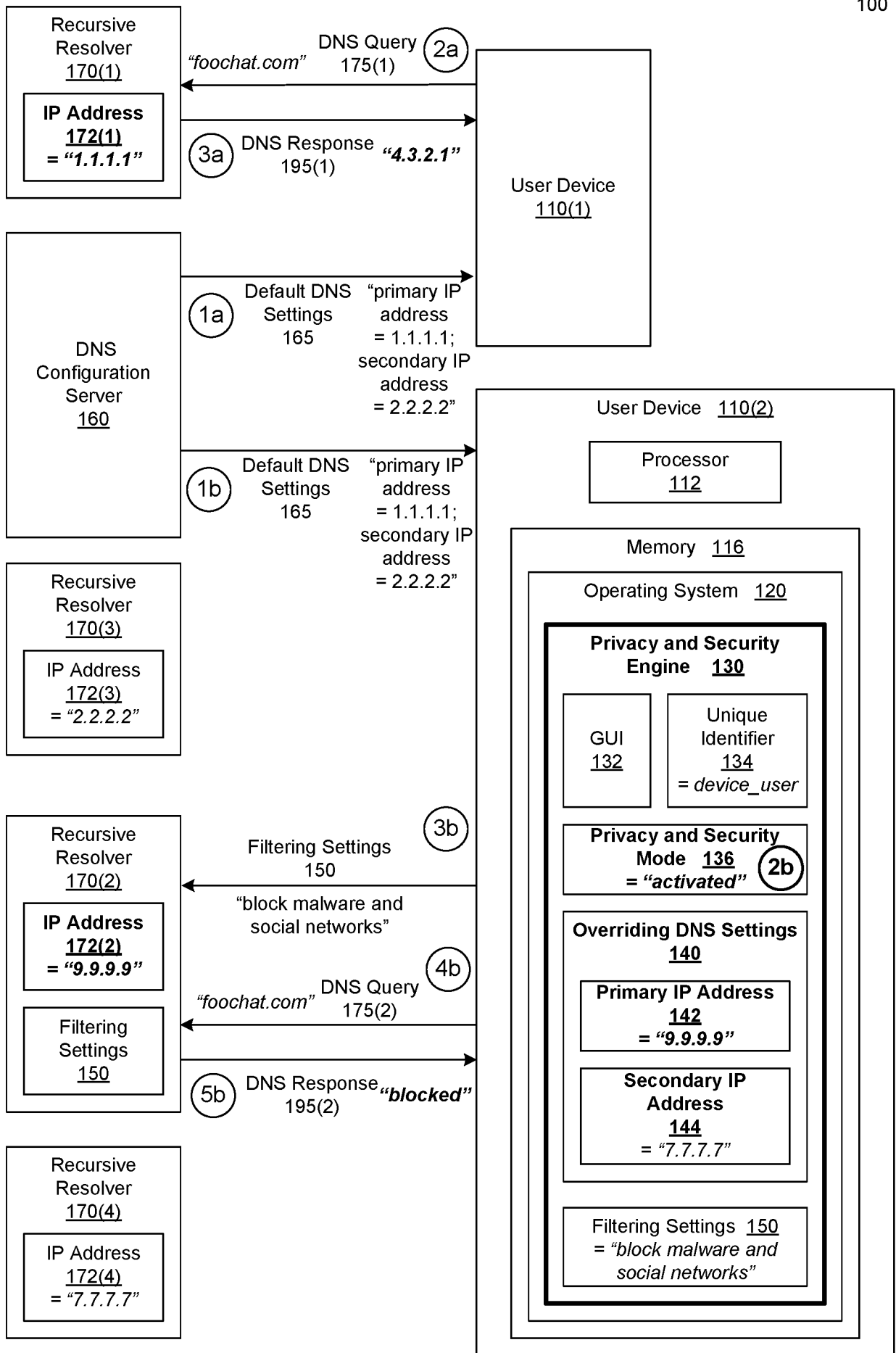


FIGURE 1



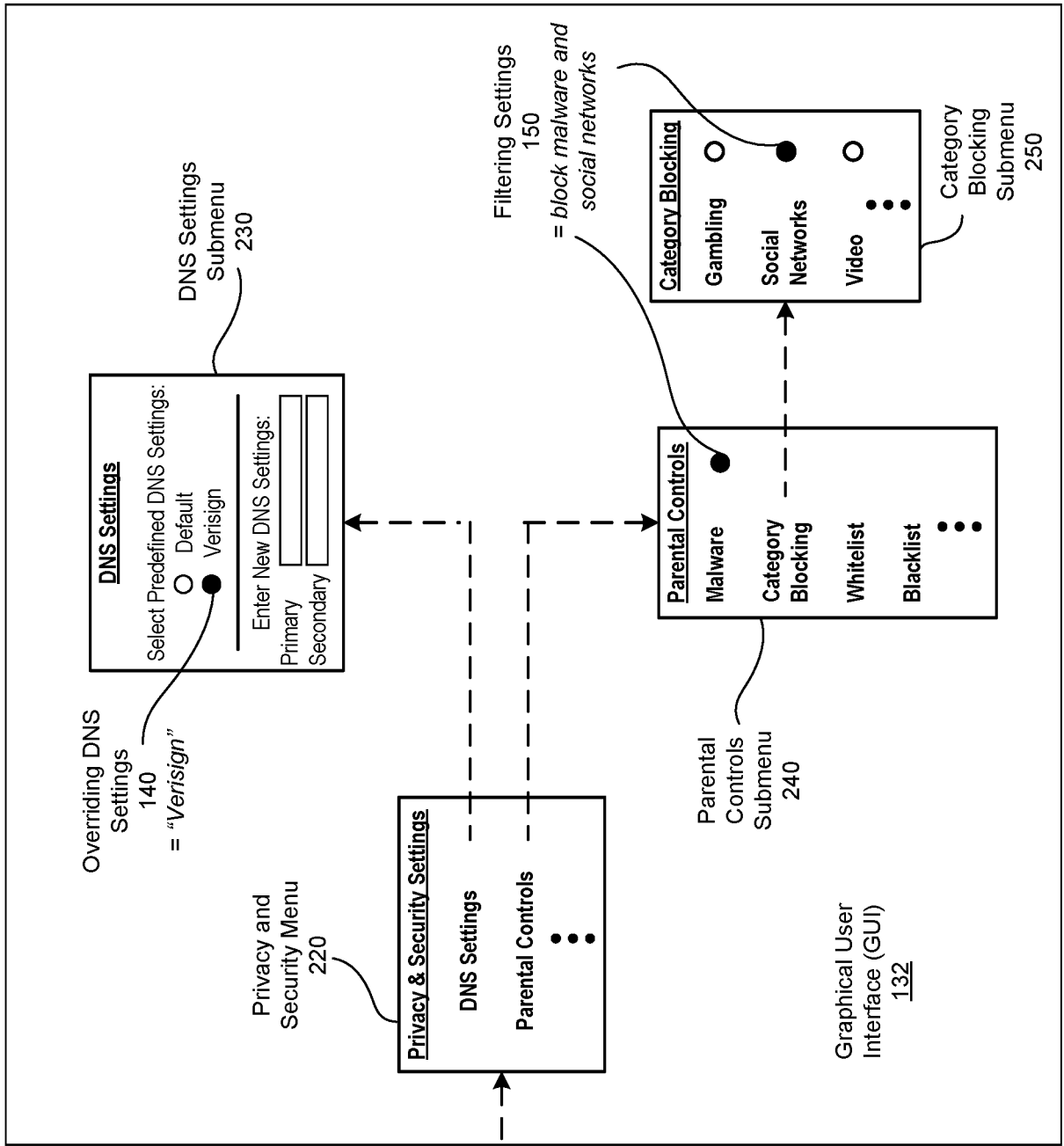


FIGURE 2

301

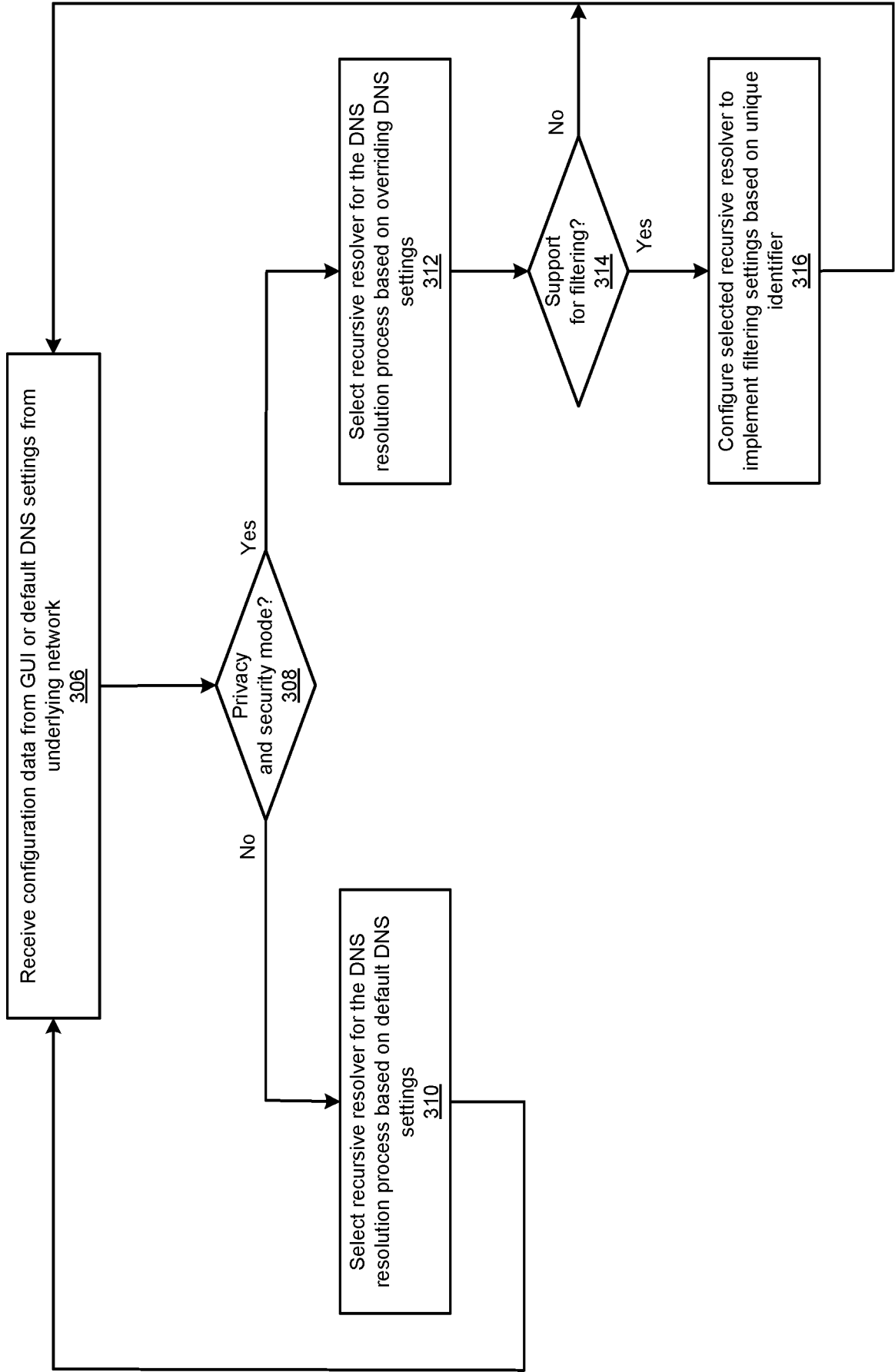


FIGURE 3

INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2016/061679

A. CLASSIFICATION OF SUBJECT MATTER  
INV. H04L29/12  
ADD.  
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED  
Minimum documentation searched (classification system followed by classification symbols)  
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Anonymous: "Set DNS", 3 October 2015 (2015-10-03), pages 1-3, XP055347858, Retrieved from the Internet: URL:http://web.archive.org/web/20151003145 236/https://play.google.com/store/apps/det ails?id=uk.co.mytechie.setDNS&hl=en [retrieved on 2017-02-20] the whole document ----- -/--	1-20

Further documents are listed in the continuation of Box C.

See patent family annex.

\* Special categories of cited documents :

<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>
---	---

Date of the actual completion of the international search  21 February 2017	Date of mailing of the international search report  28/02/2017
---	--

Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer  Nocentini, Ilario
--	---

## INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2016/061679

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>David Ulevitch: "Introducing FamilyShield Parental Controls - OpenDNS Umbrella Blog",</p> <p>23 June 2010 (2010-06-23), pages 1-3, XP055347868, Retrieved from the Internet: URL:https://blog.opendns.com/2010/06/23/introducing-familyshield-parental-controls/[retrieved on 2017-02-20] the whole document</p> <p>-----</p>	1-20
A	<p>Jack Busch: "How to Set Up OpenDNS on Your Home Network [Router Configuration]",</p> <p>25 February 2013 (2013-02-25), pages 1-10, XP055347877, Retrieved from the Internet: URL:https://www.groovypost.com/howto/setup-opendns-home-network-router/[retrieved on 2017-02-20] page 1 - page 3</p> <p>-----</p>	1-20
A	<p>WO 2009/005433 A1 (ERICSSON TELEFON AB L M [SE]; KAUPPINEN TERO ALEKSANTERI [FI]; KUPARIN) 8 January 2009 (2009-01-08) page 2, line 12 - page 3, last line</p> <p>-----</p>	1-20
A	<p>US 2009/157889 A1 (TREUHAFT NOAH [US]) 18 June 2009 (2009-06-18) paragraph [0003] - paragraph [0014]</p> <p>-----</p>	1-20

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US2016/061679

## Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2.  Claims Nos.: 1-20(partially)  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:  
see FURTHER INFORMATION sheet PCT/ISA/210
  
3.  Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1.  As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
  
2.  As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
  
3.  As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4.  No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

### Remark on Protest

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.

**FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210**

Continuation of Box II.2

Claims Nos.: 1-20(partially)

The paragraphs 70-89 of the description refers to different embodiments of the invention but are formulated using a claim tree structure. This renders the protection conferred by the claims unclear contrary to the requirements of Article 6 PCT and thus a meaningful search is possible only excluding said paragraphs from the searched subject-matter.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guidelines C-IV, 7.2), should the problems which led to the Article 17(2) declaration be overcome.

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2016/061679

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009005433	A1	08-01-2009	NONE
-----			
US 2009157889	A1	18-06-2009	US 2009157889 A1 18-06-2009
			US 2014237139 A1 21-08-2014
-----			