A method and system to manage phone call communications to individual consumer phone devices

Background

[0001] The present invention pertains to a method and system to manage phone call communications to individual consumer phone devices.

[0002] 1. Field of the invention

[0003] This invention relates generally to the detection, filtering and processing of unsolicited or undesired telephone calls to consumer (landline, VOIP, mobile or other) devices.

[0004] 2. Description of Related Art.

[0005] There are techniques available in the art for filtering, forwarding and blocking incoming telephone calls at both the Telco Carrier scale and within the consumers home using devices.

[0006] Techniques implemented by Telco Carriers are deployed across their networks and, as rule, merely compare the destination telephone number with entries on the FTC 'Do not call registry"- the DNCR. If the destination is a match, the call is dropped. US Patent No: 7,158,630 and US Patent No: 6,330,317. This prior art for suffers from one or more of the following limitations. Firstly, these techniques assume the validity of the callerID which can be spoofed (despite laws saying such action is illegal), the calls then pass the DNCR test and the call is not rejected. Secondly, these techniques place a financial burden on the consumer. The customer has to pay the Telco who deploys these solutions every month and the number of calls that can be effectively blocked in small and not simple to modify. Thirdly, the illegal callers simply adapt their calling identities so they are not recognized as nuisance callers. Fourthly, these techniques do not offer the ability to share nuisance caller data between consumers. Lastly, the DNCR is the primary filter that is applied, and the consumer has to trust (and pay blindly) hoping the carrier solution will filter out undesirables. VOIP filters for Spam Calls over Internet Telephony (SPIT) are even less evolved and more difficult to implement than callerID on POTS systems.

[0007] Techniques implemented in consumer household call blocking devices often require manual interactions with the device on every new unwanted call. These devices then typically hang up and/or play a 'fake' line is disconnected tone to the caller in an attempt to dissuade further calls to the consumer's device. Much of the prior art suffers from one or more of the following limitations. One, it is largely passive in nature. A nuisance number has to be blocked by each and every consumer receiving it. Two, those devices that do attempt to update the DNCR are subject to the same limitations of DNCR effectiveness already discussed. Three, being manual systems, they do not readily and automatically adjust to new nuisance or unsolicited caller campaigns or rapidly altering caller identities.

[0008] In short, despite the advent of the FTC DNCR and the availability of Caller ID call screening for phone numbers, a high volume of unwanted calls to consumer's land, VOIP and mobile device phones continues. Previous devices, methods and inventions have offered limited filtering and blocking options to allow consumers to choose which numbers they regard as nuisance. However, previous devices, methods and inventions have largely neglected the fact that countless websites, email lists and bulletin boards have sprung into existence where consumers ask each other for information and express dismay at the latest slew of unwanted calls.

[0009] In light of the above discussion, there is a need for a method and system to provide a dynamic, inexpensive caller identification filtering and response solution. The method and system should not simply rely on the DNCR, rather it should adapt to nuisance caller number changes as automatically as possible and it should scale and share information between consumers.

Summary

[0010] In light of the present need for a dynamic caller identification filtering and response based solution that is able to adapt to telemarketing and other nuisance caller identities as they evolve. A brief summary of various exemplary embodiments is presented. Some simplifications and omission may be made in the summary which is intended to highlight and introduce some aspects of the exemplary embodiments.

[0011] The invention is comprised of four major components, each with a unique function that operate in tandem.

[0012] A client software editor

[0013] A CPE (customer premises equipment) based device to attach to the consumers phone line (POTS or VOIP)

[0014] An Internet based server and service (IBSS) provided by a company that stores both caller identities and actions to take on those identities that are to be executed by the CPE device.

[0015] Unique proprietary software components that execute on the CPE device, on mobile communication devices and on servers comprising the IBSS

[0016] An object of the invention is to provide a method and system to process incoming caller identity information on the device that in turn performs actions specified by the customer defined on a caller identity.

[0017] A second object of the invention is to provide a method and system that enables Internet connected versions of the device to automatically acquire lists of nuisance numbers ('blacklists') from suitable disparate Internet connected servers and services to augment locally edited consumer defined action caller identity lists.

[0018] A third object of the invention is to provide a method and system that enables Internet connected versions of the device to automatically share it's list of nuisance numbers ('blacklists') to the IBSS if the consumer wishes.

[0019] A fourth object of the invention is to execute programmatic code on the IBSS to aggregate, clean, weight and provide near real-time blacklists of nuisance numbers; so as quickly as the illegal or nuisance callers alter their calling identities, the IBSS makes that data available to those consumers with internet connected devices.

[0020] A fifth object of the invention is to enable Internet connected versions of the device to be able to reply to incoming calls not with a simple a tone response, or hangup, but with consumer defined Internet protocol messaging such as, but not limited to, Email and SMS-Text messaging.

[0021] A sixth object of the invention is to enable consumers who cannot or choose not to connect their device to the internet to provide 'blacklists' in a common data format such a "tab delimited text" directly to their device via a USB memory stick, thereby enabling processing of incoming caller identities with the file so provided. Such device configurations would only be able to block or pass the call.

[0022] A seventh object of the invention is to provide a robust cross-platform editing tool to permit consumers to create action lists to process incoming caller identities and store this information on the IBSS, and should they so wish, share their private blacklist with others through the IBSS.

[0023] An eighth object of the invention is to enable Internet connected versions of the device to download copies of aggregated databases to local storage to permit faster comparison of incoming caller identities with the private consumer database and blacklists created through the aggregation, cleaning and weighting of social-crowd media submitted nuisance numbers to the IBSS.

[0024] The overall design provides novel and improved methods to redress both illegal and nuisance calls that consumers identify as impacting their lives in a negative manner. It extends possible responses to incoming calls enabling the consumer to transmit Internet protocol based notifications to numbers with identifiable email or SMS text contact information associated with them via the CPE device.

[0025] The client software editor identified is written to run on specific versions of the Microsoft Windows, Apple MacOS and Linux. It can also be executed on suitably enabled Google Android devices and Apple IOS devices. The editor provides a consistent look and feel across these platforms. The editor is required to access and manage the consumer's private CallerID and actions data hosted on IBSS managed databases, Figure 4.

[0026] The editor interface authenticates the consumer account on the IBSS Figure 4 and permits the editing of caller identities (numbers) and related actions and store this information on an IBSS managed database 440.

[0027] The editor permits the consumer to download their entire collection of caller identity-action combinations from the database 440 and store the data in a well specified folder-directory in a file with a specific name, in a specific format, on the consumer's computer or mobile device executing the data editor.

[0028] The CPE device extracts incoming POTS caller identities such as E164 standard phone numbers using a hardware based micro controller and software running under Linux, proprietary software also isolates URIs that are part of a VOIP data Internet Protocol packet.

[0029] The incoming caller identity is compared to a list of identities stored in a database on the CPE device and an action is taken if the number is matched. If a number is not matched it is passed through the system. That is, a number (caller identity) is 'white listed' until it is explicitly not.

[0030] The Internet based server and service, IBSS, provided by a company, runs proprietary code that is part of this invention. It stores both caller identities and actions to take on those identities that are to be executed by the CPE or mobile communications device. The same entity, IBSS, provides this client side proprietary code that is a part of this invention.

[0031] The IBSS stores data on an per registered user account basis and this data is visible and accessible for edit via the Internet using the account holder's login credentials that are created and maintained on the IBSS [14]

[0032] The IBSS runs proprietary code that is part of this invention that enables it to access specific Internet sites such as, but not limited to, social-crowd media sites to aggregate, clean and weight data on nuisance numbers posted by individual consumers. Customers would share these potential nuisance caller identities using methods they are already familiar with. This data is then presented via the Internet using methods familiar to those versed in the art to both CPE and mobile devices of other consumers.

[0033] This data, accessed directly over the Internet or copied to the consumers device of choice would augment the private local database information created via methods such as the CPE editor.

[0034] Having multiple sources of nuisance caller data and multiple ways in which consumers can access this data makes it more difficult, and expensive for those determined to impinge upon the privacy of others to continue doing so.

[0035] The subject matter discussed herein describes a system and method whereby a consumer can automatically block unwanted phone calls to their legacy POTS, VOIP or mobile communications devices. The system and method describes how a consumer can blacklist numbers (caller identities) they do not want and how they can then dynamically share their blacklisted numbers from their private local database with one or more aggregated, cleaned, weighted public databases that represent a dynamic and fast evolving list of nuisance callers. This sharing of data leverages both familiar Internet social-crowd media tools (Apps) on mobile consumer devices and the consensual sharing of private blacklists from the CPE device housed behind the Demarc of private residence or business.

[0036] For any blocking solution to be effective and to scale two things must happen.

[0037] Firstly, the consumer has to decide what incoming phone calls are a nuisance, in the same way as he/she does in deciding what incoming Email is SPAM. Today a consumer sets up filters in Email to help whittle down nuisance Email and ISPs (Internet Service Providers) do the same using numerous methods including black and white list databases to block (Email) spammers. This process has enjoyed considerable success as the consumer has the final say in what constitutes unwanted (nuisance) Email. It

has also been successful because an analysis of the Email structure helps 'weight' it's likelihood of being SPAM using both statistical methods and direct 'mark as junk' flagging by the consumer.

[0038] Secondly, consumers must be able to (if they so wish) dynamically and easily share their private blacklisting data with millions of consumers at large - in (pseudo) real time and have this data easily accessible by all consumer devices that can receive phone calls.

[0039] Unfortunately, even with the advent of the "Do Not Call Registry" (DNCR) and U.S. legislation making it illegal to forge CallerIDs, the number of unwanted calls and registered complaints with the FTC continues to rise. Having telemarketers 'register' has been a minimal deterrent to an increasing volume of calls surging past the DNCR when potential profits outweigh potential fines. To make the situation worse, it is all to easy to forge VOIP header information that masks the callers identity. So, consumers keep registering increasing volumes of complaints year on year and yet the intrusions into privacy continue largely unabated.

[0040] The system and method here tackles this problem in a novel manner of several fronts.

[0041] Instead of allowing the Telecommunications industry to charge monthly fees for static number blocking and expecting the government to offer anything more than the DNCR, the system and method here permits a consumer to define any incoming call as a nuisance and even share their data dynamically to a larger environment where aggregate, near real time updated databases share out blacklists to anyone choosing to use them.

[0042] By doing this, as fast a nuisance callers alter their identities, these larger databases reflect those changes and allow the consumer to reference BOTH their own world view of nuisance AND a larger social media-crowd view of nuisance callers.

[0043] This is in effect a feedback loop. No longer is the consumer restricted to his own well defined blacklists. He/she can also leverage the aggregate experiences of millions of people sharing their lists. This provides an adaptive blacklisting solution that does not rely on telemarketing registrations, more legislation and costly recurring monthly Telco charges.

[0044] It is elegant, in that official databases accessible by the public could be derived from these aggregate social-crowd progenitors and more conservative consumers could then have a choice of blocking using a combination of [a] their own private local database [b] a social-crowd aggregated, weighted, cleaned database or [c] Official (FTC?) blacklist databases that are consumer facing and accessible directly via authentication (unlike the DNCR).

[0045] Implementations of the above aspect may include one or more of the following.

[0046] Various aspects and embodiments of the invention are described in further detail below.

Brief Description

[0047] The present invention described herein will become apparent from the following detailed description considered in connection with the accompanying drawings, which disclose several embodiments of the invention. It should be understood, however, that the drawings are designed for the purpose of illustration and not as limits of the invention.

[0048] FIG. 1 shows an exemplary environment in which the CPE device operates in accordance with an embodiment of the disclosed invention.

[0049] FIG. 2 is a second exemplary embodiment showing a possible mode of operation of the CPE device in block diagram form.

[0050] FIG. 3A is a flowchart outlining the high level operation of the method and system in accordance with one or more embodiments of the invention.

[0051] FIG. 3B is a flowchart outlining caller identity extraction (decode) and storage in accordance with one or more embodiments of the invention.

[0052] FIG. 3C is a flowchart outlining how stored calling identities are compared to the local private CPE and other databases in accordance with one or more embodiments of the invention .

[0053] FIG. 3D is a flowchart outlining what actions are performed on identities stored in the CPE device buffer in accordance with one or more embodiments of the invention.

[0054] FIG. 3E is a flowchart showing what data from action executions is logged and shared in accordance with one or more embodiments of the invention.

[0055] FIG. 4 is a flowchart showing what public databases are created and how data is uploaded to them in accordance with one or more embodiments of the invention.

[0056] FIG. 5 is a flowchart showing how the CPE editor populates the consumer private database on an IBSS environment in accordance with one or more embodiments of the invention.

[0057] FIG. 6 is a schematic showing how CPE or mobile communication devices can download blacklist data to local databases in accordance with one or more embodiments of the invention.

Detailed Description

[0058] FIG. 1 shows an exemplary environment in which the CPE device operates in accordance with an embodiment of the disclosed invention.

[0059] The CPE device 124 resides behind the Demarc 116 in customer premises 118. The CPE device 124 processes incoming VOIP 122 or legacy POTS 120 calls. The flow of calls into the CPE device 124 is considered from the Telecommunications carrier network 100 via their Central Office 102 with it's Spam blocking layers 104 and 106, via a converged phone access network 108 and in from street Utility boxes 110 is shown. Both POTS 112 and SIP 114 data cross the Demarc 116, in the simplest scenarios, on the same single loop from the carrier.

[0060] FIG. 2 is a second exemplary embodiment showing a possible mode of operation of the CPE device in block diagram form

[0061] The CPE device 200 is an embedded computer system capable of running a modern multi-threaded operating system and numerous Opensource application software components in addition to proprietary software that is a component of this invention whose function is disclosed in Figures 3A-3E and elsewhere herein.

[0062] The CPE device 200 comprises an MMU enabled central processing unit (CPU) 226 with access to both volatile random access memory (RAM) 228 and nonvolatile RAM 230 and to external data storage such as USB memory 234 through an IO subsystem 232.

[0063] The nonvolatile RAM 230 is the repository for the operating system, the local private blacklist database 220, Opensource applications, any partial or complete copies of shared blacklist databases downloaded from the Internet and the proprietary software that is part of the invention.

[0064] The local private database 220 is created and updated using either a data editor who's function is part of the disclosed invention or using a commonly available text editor or lastly, by proprietary code

that is a component of the disclosed invention and who's function is described in an exemplary manner in Figure 6.

[0065] The CPE device 200 is able to accept, process and take actions when receiving either POTS or VOIP calls using the proprietary software executing upon it. Mobile devices execute the same proprietary code matched to their own particular operating system.

[0066] Incoming POTS type calls enter the CPE device 200 from the local phone loop 202 via a standard telephone connector 236, similar to an RJ11/RJ14 and are passed to the start of the CPE solution stack 210 at the decode layer 212.

[0067] At the decode layer 212, the CallerID is stripped from the incoming call from the Telco Central office 102 between the first and second rings using a commonly available microprocessor based circuit described in prior art. The CallerID 316 , or a code indicating a decode issue was encountered 320,324 is stored in a buffer 238 where it is accessible to the proprietary code whose function is described in Figures 3A-3E.

[0068] Incoming VOIP type calls are intercepted by the CPE device 200 through one of two Local Area network (LAN) RJ45 network connections 206 and are passed into the CPE solution stack 210 at the decode layer 212. Proprietary code that is part of the invention executing on the CPU 226 examines and dissects Internet Protocol packets looking for SIP invitations and it strips caller identification from this. The isolated caller identity is stored in a buffer 238 where it is accessible to the proprietary code whose function is described in Figures 3A-3E.

[0069] FIG. 3A is a flowchart outlining the high level operation of the method and system in accordance with one or more embodiments of the invention

[0070] The CPE device 200 waits for an incoming POTS or VOIP call at Call Start 300.

[0071] When the consumer is receiving a POTS call the decode layer Figure 3B, 316 attempts to extract the CallerID between the first and second rings using technology presented in prior art and proprietary

software and store this identity, or a code indicating a private call or failed decode into the buffer 238,302. Incoming VOIP calls have their identities extracted using proprietary code executing on the CPE device 200 that examines Internet Protocol packets directly via network interface-1 206.

[0072] The buffer 238 is compared with a consumer defined combination of local private database 220 and remote databases of blacklisted identities/numbers 304.

[0073] Consumer defined actions 306 to instantiate on the incoming call are now executed by proprietary software as defined by the rules within the local 220 or remote database.

[0074] The actions can include, but are not limited to, a hang-up (go on-hook) signaled to POTS calls via the hardware within the decode layer Figure2, 212 or a drop of the SIP invitation packet by the proprietary software running on the CPE device 200 (thereby hanging up on the incoming VOIP call)

[0075] Lastly, the proprietary software logs 308 all it's actions locally to nonvolatile RAM 230 and if the device 200 is connected to the internet, the consumer can opt to share logging activity.

[0076] After logging is complete and the call has either been passed through the system for answering or 'hung up' on, the system and method returns to call Start 300 to await a new incoming call.

[0077] FIG. 3B is a flowchart outlining caller identity extraction (decode) and storage in accordance with one or more embodiments of the invention

[0078] This shows how a new incoming Call Start 300 has the caller identity stripped and stored in a buffer 238.

[0079] The decode layer 212 is aware through a combination of hardware and proprietary software how a call should be decoded 314. If the decode layer detects an 'off-hook' event then a calling number identification circuit similar to one disclosed in prior manufacturers art attempts to isolate the CallerID between the first and second rings.

[0080] If the proprietary software detects incoming SIP information it is extracted 312 from network interface-1 206.

[0081] If it is a private caller 318 a special code 320 is set in the buffer 238.

[0082] If the caller identity fails to decode to a CallerID 316 or SIP caller identity 312 a special code is set 322 in the buffer 238.

[0083] On a mobile device the same algorithm is applied to the last caller number received instead.

[0084] The decode layer described in an exemplary manner here can be perceived as a shim between the proprietary software and input from the physical world. This software - hardware layer can be modified as needed so long as a suitably formatted buffer 238 is set and made available to later stages of the solution stack 210.

[0085] With the caller identity or the state of the attempted decode now stored in the buffer 238, the proprietary software proceeds to see if the consumer has any actions to take upon matching this identity or code. This is described in Figure 3C.

[0086] FIG. 3C is a flowchart outlining how stored calling identities are compared to the local private CPE and other databases in accordance with one or more embodiments of the invention

[0087] This shows how the CPE 200 or other device compares the buffer 238 with databases 220 local to the device.

[0088] Furthermore, if the device is internet connected via network interface-2 208 the buffer 238 can be compared with one or more Internet hosted blacklist databases Figure 4, 350. The remote database(s) internal structure of caller identities and actions is accessible and compatible with the CPE 200 device using standard Internet based remote database access techniques familiar to those experienced in the art.

[0089] At all times actions defined in the private local database take precedence over actions defined elsewhere 442,446,448. This remains true whether device accesses data originating from remote databases over the Internet directly Figure 6 or via complete or partial copies of remote databases migrated to the local device nonvolatile RAM 230.

[0090] Consequently, any caller identity and actions in the local private database set to non-Block is effectively a white-listed caller identity.

[0091] The device proprietary software reads the caller identity from the buffer 238. If that value represents a private call 332 or a failed caller identity decode 334 then the call immediately proceeds to the actions stage 340 defined in Figure 3D.

[0092] If the buffer 238 is matched in a local private database 336 the call is passed on to the actions stage 340 defined in Figure 3D.

[0093] What happens next 342 in the proprietary software of an Internet connected 338 device is a major differentiator between this invention from other prior art

[0094] An Internet device sets an expiry timer 346 and then attempts to match the buffer 238 with one or more Internet based 348 databases of blacklisted identities. If the buffer 238 is matched 350 the call is passed on to the actions stage 352 defined in Figure 3D.

[0095] If the buffer 238 is not matched before the timer expires 354 the call is passed on 356 to the actions stage 352 defined in Figure 3D with an expiry state recorded.

[0096] Devices initiate the comparison of buffer 238 over the Internet with remote databases using access techniques familiar to those experienced in the art.

[0097] Devices can also compare the buffer 238 with data downloaded from a remote database to nonvolatile RAM. This reduces latency in deciding whether or not to block the incoming call. The remote data structure and access methods are described in an exemplary manner in Figure 4. Functions within the proprietary software facilitate the download of this data Figure 6.

[0098] The buffer 238 is now available to the actions layer Figure 3D

[0099] FIG. 3D is a flowchart outlining what actions are performed on identities stored in the CPE device buffer in accordance with one or more embodiments of the invention

[0100] The actions a CPE or mobile device running the proprietary code can take using the buffer 238 as a key into the database are now described.

[0101] The actions layer is instantiated 358 from the process layer Figure 3C. In this exemplary flow if the buffer 238 is matched directly 360 on a remote database the proprietary code simply sends an on-hook or drops the SIP invitation packet terminating the incoming call 374.

[0102] If the buffer 238 is either code1 318 (*67 private) or code2 322 (caller identification decode failed) the identity of the caller could not be ascertained and by default the incoming call is passed 362 (no hang up issued) but no other actions are performed.

[0103] If the buffer 238 is matched in a PRIVATE local database the customer can elect to block/not-block 372 the call and to send electronic mail 364 or SMS text messages 368 to Internet locations using standard Internet protocols 366,370 associated with the owner of the identity 238.

[0104] If the buffer 238 is matched on a database local to the device that was derived from a third party 442,446,448 database, proprietary code simply sends an on-hook or drops the SIP invitation packet terminating the incoming call 374.

[0105] After an incoming call has been processed and all associated actions instantiated (Figures 3A-3D) the actions layer is complete and the proprietary software moves on to the final phase, logging and data aggregation layer Figure 3E.

[0106] FIG. 3E is a flowchart showing what data from action executions is logged and shared in accordance with one or more embodiments of the invention

[0107] Logging behavior the CPE device 200, or any other mobile device with access to the IBSS managed environment 458 can take is discussed here.

[0108] The arrival time of an incoming call, the decoded buffer 238 and all actions taken are logged to nonvolatile RAM 230 local to the device 378, 380.

[0109] If the CPE 200 or mobile device is internet connected 208 then Email the activity log on a schedule set by the consumer 384.

[0110] If the consumer has given consent then activity logs can be shared anonymously 386 and uploaded 388 to the IBSS managed 458 environment using methods familiar to those with experience in the art.

[0111] An exemplary description of the function and operation of this secured access but publicly accessible Internet service (IBSS) is disclosed and described in detail in Figure 4 and is an embodiment of the invention.

[0112] With the logging layer complete, the proprietary software now waits for a new call 390 (Figure 3A)

[0113] FIG. 4 is a flowchart showing what public databases are created and how data is uploaded to them in accordance with one or more embodiments of the invention

[0114] This schematic showing shows what publicly accessible databases are created containing blacklisted caller information , how data is populated (uploaded) into them and explains the dynamic nature of the blacklisting process. As quickly as nuisance callers alter their identities, one or more of these databases will present data back to consumers who can then choose which database (in addition to their local private database) can supplement a dynamic worldview of nuisance caller identities.

[0115] Numerous data source entry points for blacklist candidate callerID data for the individual private database 440 records and aggregated databases 442 are envisioned by the invention.

[0116] These include, but not limited to, the CPE editor 402 ,Figure 5 , mobile communication devices 'Apps' 404 and Internet Web browsers 406. Each entry point requires a Strongly Authenticated Login 452 via a registered account on the IBSS managed 458 environment to permit the consumer to submit 412 a potential caller identify for blacklist processing 418,424,428.

[0117] Strongly Authenticated Login 452 for submissions is suggested because data accepted here will be used to populate the CPE 200 or any mobile device local blacklist private database records 440 and the aggregated database 442.

[0118] Potential blacklist identities are submitted 412 to the IBSS managed databases 440,442 over the Internet using methods well known to those familiar in the art.

[0119] If a submitted 412 blacklist identity 418 is accepted 424 as a candidate then it is written to the consumers private database records 440 if it does not already exist.

[0120] If the blacklist identity does not exist in the aggregated database then it is added as a new entry, the time stamp at which this occurred is set and the number of occurrences of this entry is initialized to one. This mechanism happens via what is termed here as a split-write 428,432

[0121] If the blacklist identity does exist in the aggregated database 442 then the time stamp of the existing matched entry is updated and the number of occurrences of this entry is incremented by one.

[0122] This aggregate database 442 therefore reflects a 'world view' of what consumers deem nuisance calls. The number of occurrences of a blacklisted identity provides an indication of how 'annoying' that caller identity has been over time and the time of day stamp on the record indicates if it's a current, ongoing 'attack' from that particular number or, as the time stamp gets older, represents a nuisance caller identity that is not currently 'active'.

[0123] By comparing the total number of occurrences per identity and last time a caller identity has been blacklisted by consumers, devices can query directly over the internet 348 during an incoming call and see if the incoming call originates from current a trending nuisance caller identity.

[0124] The consumer can instead opt to have their device download a defined portion of the trending aggregate 442 or social-crowd 446 databases over Internet on a schedule of their choice to local device storage and query the buffer 238 locally for better response times.

[0125] The preceding discussion in this section constitutes a novel and dynamic method to permit consumers to identify and share nuisance caller information as they have never done before.

[0126] However, consumers who do not wish to filter their calls using a device can still contribute received nuisance call identities simply and dynamically to social-crowd 446 databases using social-crowd media tools. Once again this leads consumers down the familiar path of trending data for nuisance calls.

[0127] One such social-crowd data source could be, but is not limited to, Twitter 408. A customer uses a simple mobile App to tweet 414 the selected offending caller identity 420 to a Twitter account specifically created to receive "sender-time-nuisance" identity tweets .

[0128] The trustworthiness of such data 454 is not as high as information submitted by a Strongly Authenticated Login 452 via the IBSS managed sources 402,404,406. However, such tweets can be cleaned, weighted and stored in a social-crowd database 446 using proprietary algorithms that are part of this invention running on an IBSS managed environment 458.

[0129] Extracting data from , or pushing data to this social-crowd database 446 from the IBSS aggregate database 442 would happen along a secured inter-database link (or social bridge) 444 using proprietary algorithms running on the IBSS managed environment 458.

[0130] The final exemplary data source identified herein is the third party input interface 410 and public facing third party database 448.

[0131] Nuisance caller identities can be added 416 and filtered 422 here by numerous private (non IBSS managed environment 458) entities or government agencies using their authentication mechanisms 456. Such databases would have to present their data such that it could be consumed by the CPE 200 or

mobile device in exactly the same manner as data from IBSS managed environment 458. This would ensure simplicity, security, scalability and usability.

[0132] In all cases described above the consumer would have to agree not to mine or attempt to manually or programatically trawl through blacklists specific to the database to which they connect as that would breach their end user license agreement (EULA) and most probably (for data in the United states) the DMCA (Digital Millennium Copyright Act) and the Computer Fraud and Abuse Act.

[0133] FIG. 5 is a flowchart showing how the CPE editor populates the consumer private database on an IBSS environment in accordance with one or more embodiments of the invention

[0134] Devices create their private local databases data 440 hosted on an IBSS managed environment Figure 4 using the client software editor. This editor performs identical functions with a similar look and feel across suitably enabled Microsoft Windows, Linux, MacOS, Apple IOS and Google Android platforms.

[0135] The editor performs two primary functions. Firstly, it manipulates data stored on IBSS managed databases Figure 4 and secondly it manages downloads of current account caller identity actions data.

[0136] The consumer installs the editor and invokes it 500. The editor requires a Strongly Authenticated Login 452 to an IBSS account registered by the consumer at an earlier date 502. The proprietary account registration and account maintenance software executed on the IBSS environment is not discussed nor disclosed herein as it's functions are familiar to those experienced in the art.

[0137] After successful login to their registered account the consumer can perform several operations on entities within their private database 440 records.

[0138] Actions defined in this private local database take precedence over all others.

[0139] Even if a device references an aggregate 442, social 446 or third party 448 database after it's local private database and detects a conflicting action for the caller identity in question, these actions are superseded by those already extracted from the local private database.

[0140] Any caller identity entered in this local private database and set to non-Block is effectively white listed.

[0141] A new caller identity and actions Figure 3D to take if it is matched in the buffer 238 can be entered 504,506.

[0142] The consumer can also elect to send Email or SMS text with a defined message to this new caller identity record 506.

[0143] The consumer can instead edit an existing 508 identity record 510 and update the actions.

[0144] The consumer can instead delete all information for an existing 508 identity record 510.

[0145] When the consumer is finished editing or deleting caller identity records 512 they can download their data to their desktop or device by logging off the IBSS server 514. A complete copy of their current private database records from the IBSS managed database 440 is extracted, compressed and automatically copied as a text file to the computer or mobile device executing the editor.

[0146] The integrity of their data download is verified 516 and notifications displayed.

[0147] This datafile can be copied to a USB stick 612,622,626 and inserted into a CPE device 200 where proprietary software reads this data and creates a new private local database for the CPE device 200.

[0148] On a mobile device this datafile will be detected at the end of it's download and be converted automatically into a new local private database.

[0149] FIG. 6 is a schematic showing how CPE or mobile communication devices can download blacklist data to local databases in accordance with one or more embodiments of the invention

[0150] The flow of layer 3 Internet Protocol data between devices and databases containing blacklist caller identities and actions is now discussed in an exemplary manner.

[0151] One example shows the CPE editor running on a computer 612. The computer communicates over it's connection 614 with the Internet 616 to an IBSS managed database 600. This database presents

Strongly Authenticated Login 452 access to it's data via a TCP encrypted Web services layer 604,608 in a manner familiar to those experienced in the art.

[0152] The consumer modifies records in the IBSS database 600 using the CPE editor Figure 5 over this encrypted channel to the database until all changes have been committed.

[0153] When the consumer elects to log off, their current private caller identity actions data is copied through the web services layer 604, 608, down their connection 614 and is stored on the computer 612. This data is copied by the consumer to a USB storage device 622. When the USB storage device is inserted into the CPE device 626 USB port 628,234 proprietary software running there automatically generates a new private local database 624. This particular local database contains only private data entered by the consumer along with actions selected for each identity (if any).

[0154] An Internet connected 618 CPE device 626 is capable of sending Email and SMS text to addresses belonging to particular caller identities Figure 3D via it's internet link 618.

[0155] An Internet connected 618 CPE device 626 is also capable of sending Email reports of it's activities executed per instructions in it's local database 624 to the registered account owners email address.

[0156] An Internet connected 618 CPE device 626 is capable of downloading third party database 602 blacklist data presented using a secured web services layer 606,610 to augment the CPE editor private local blacklist database. The design and mode of operation of this third party web services layer 606,610 would permit the same proprietary software running on the CPE device 626 or mobile device 630 that accesses IBSS managed data to access this database 602.

[0157] The mobile device 630 executing the CPE editor offers the same functionality as the editor running on more traditional Windows, MacOS or Linux computer 612.

[0158] However, the proprietary code running on the mobile device detects the arrival of a downloaded file from a remote database 600,602 and immediately creates a local database from this. There is no copying of data to/from a USB device.

Abstract

[0159] Exemplary designs for customer premises equipment (CPE) and suggested methods are provided herein for identifying , filtering and taking actions based on a calling party's telephone (POTS or VOIP) identity to a called party. The CPE (or mobile) device compares calling identities with a local private, and remote databases of blacklist numbers and then blocks and responds to these numbers using standard internet protocols. The local private database is maintained by the customer using a client editor program whose function is disclosed in an exemplary manner herein, or by using a simple datafile generated using a text file editor or spreadsheet editor. The CPE device can operate in two modes. Internet connected and non-Internet connected. An Internet connected CPE (or mobile) device can also consult remote databases of blacklisted numbers (for instance robocall numbers) using standard Internet web based methods and protocols familiar to those experienced in the art. Such Internet based databases would be created using aggregated, cleaned and weighted posts from social-crowd media submissions using proprietary code, and from individual private database information shared with the customers consent.

Figure 1 – call traversal summary

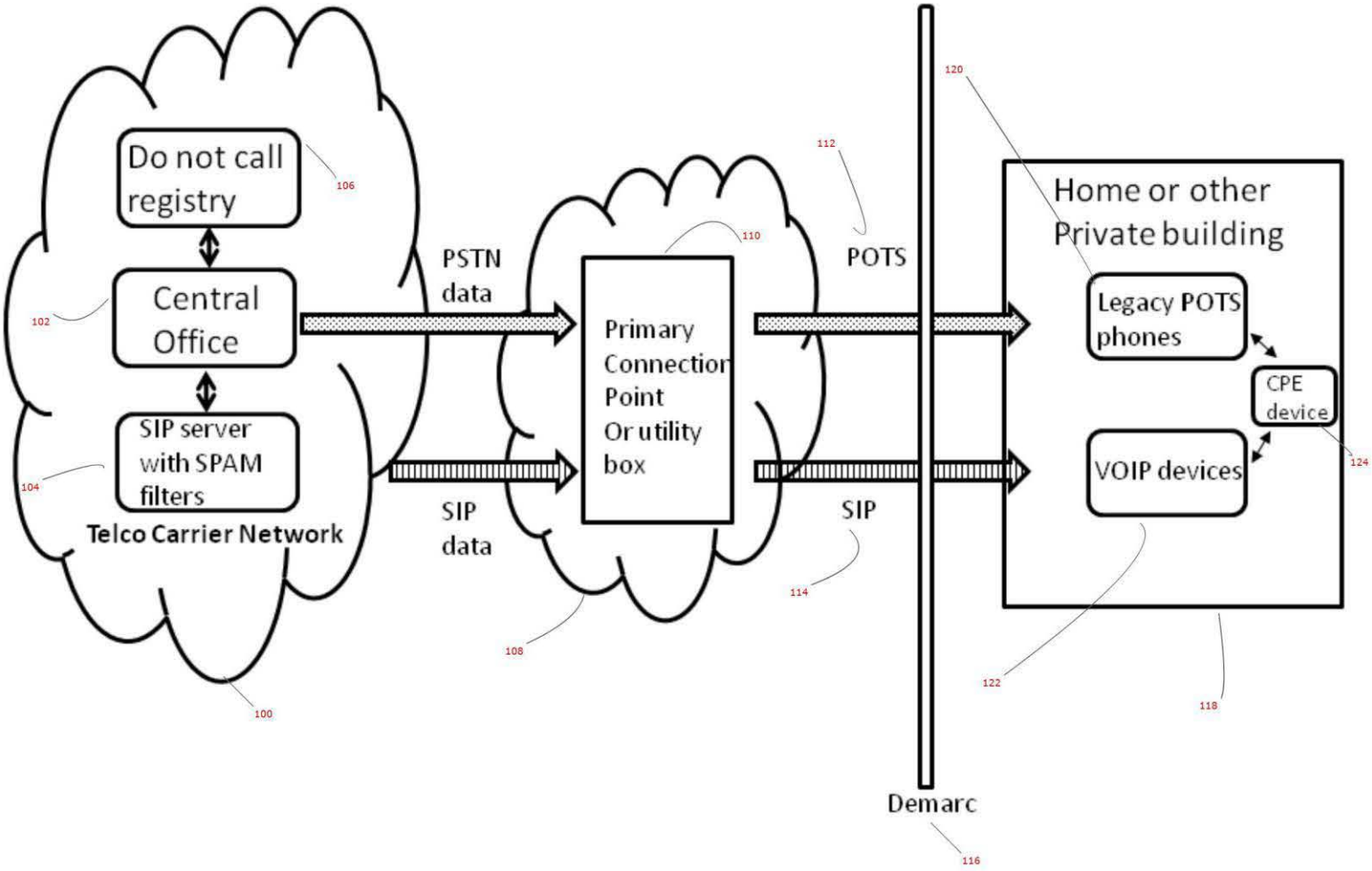

FIG. 1

Figure 2 – CPE device

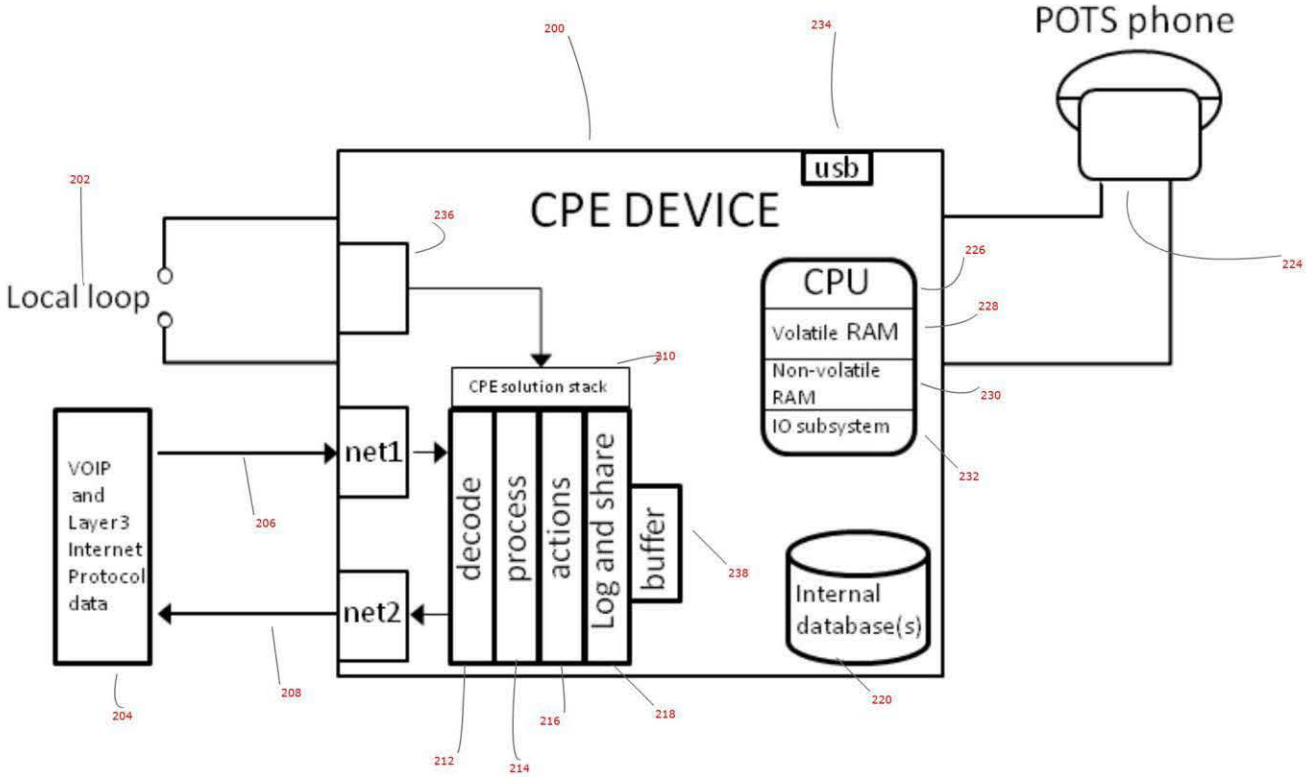

FIG. 2

Figure 3A– process flow summary

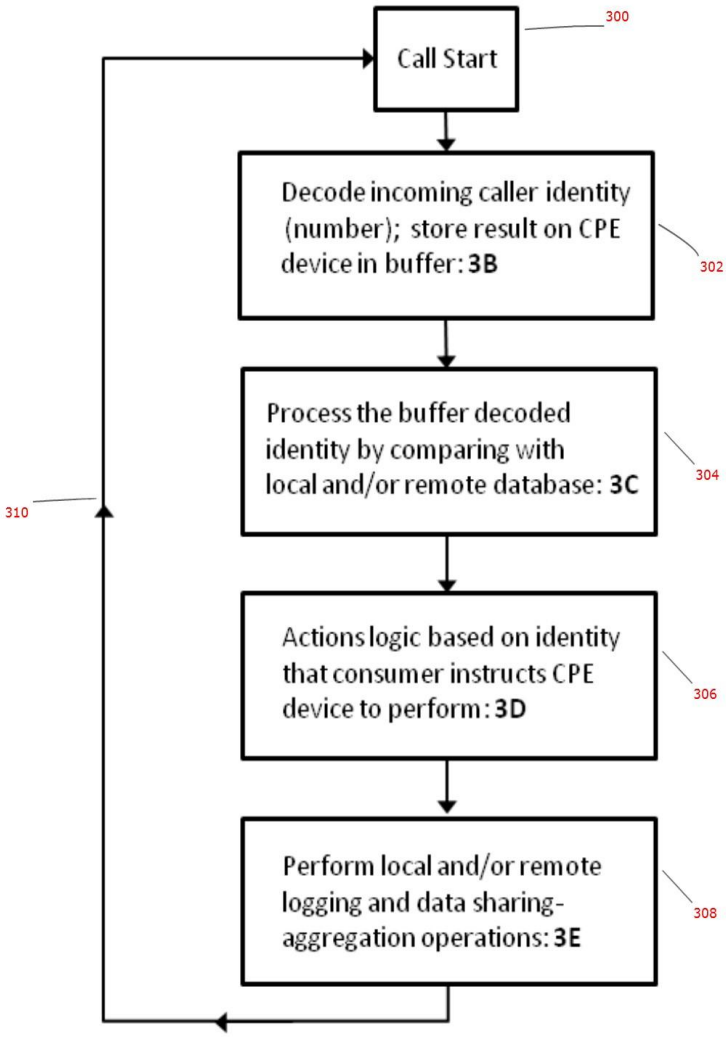

FIG. 3A

Figure 3B – Decode caller identity (number) layer

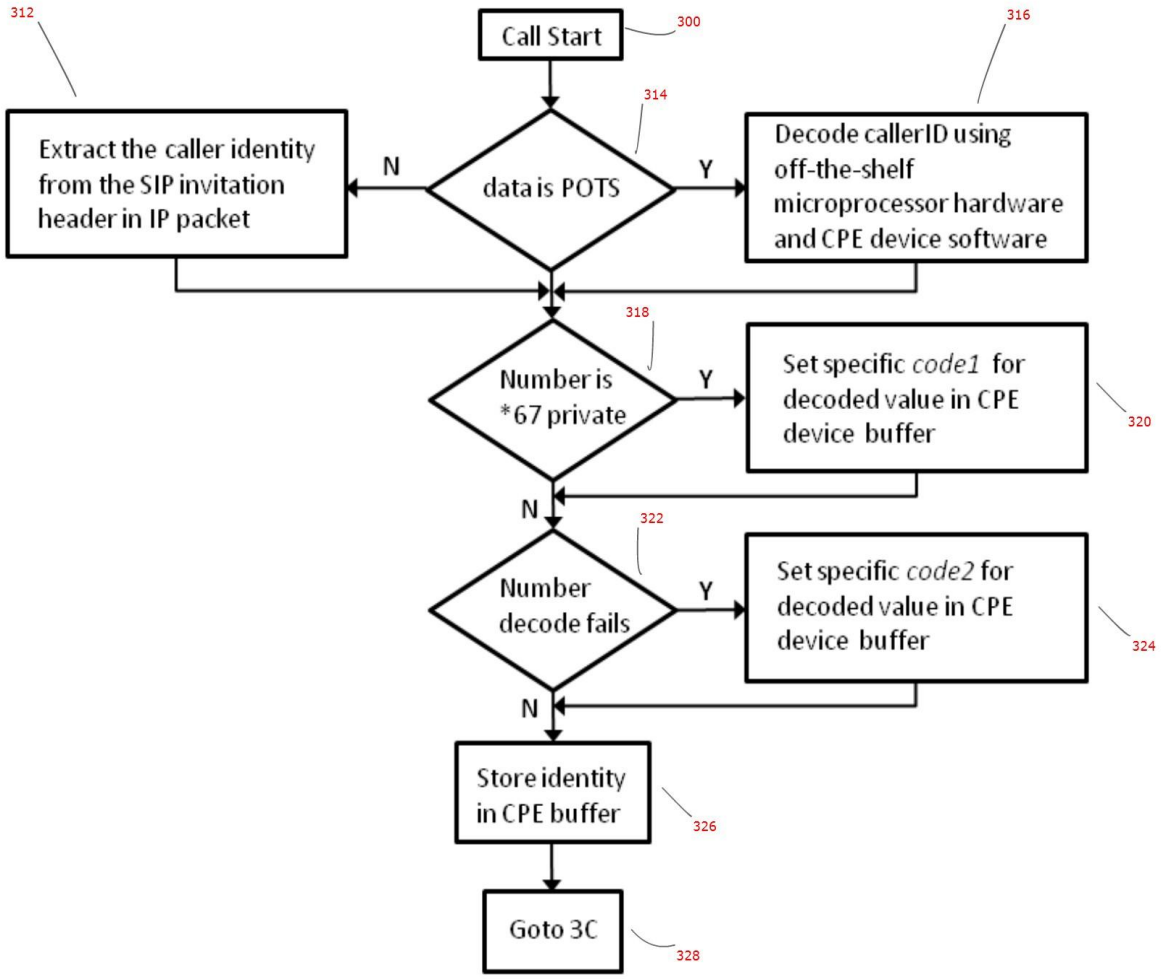

FIG. 3B

Figure 3C – Process decoded caller identity layer

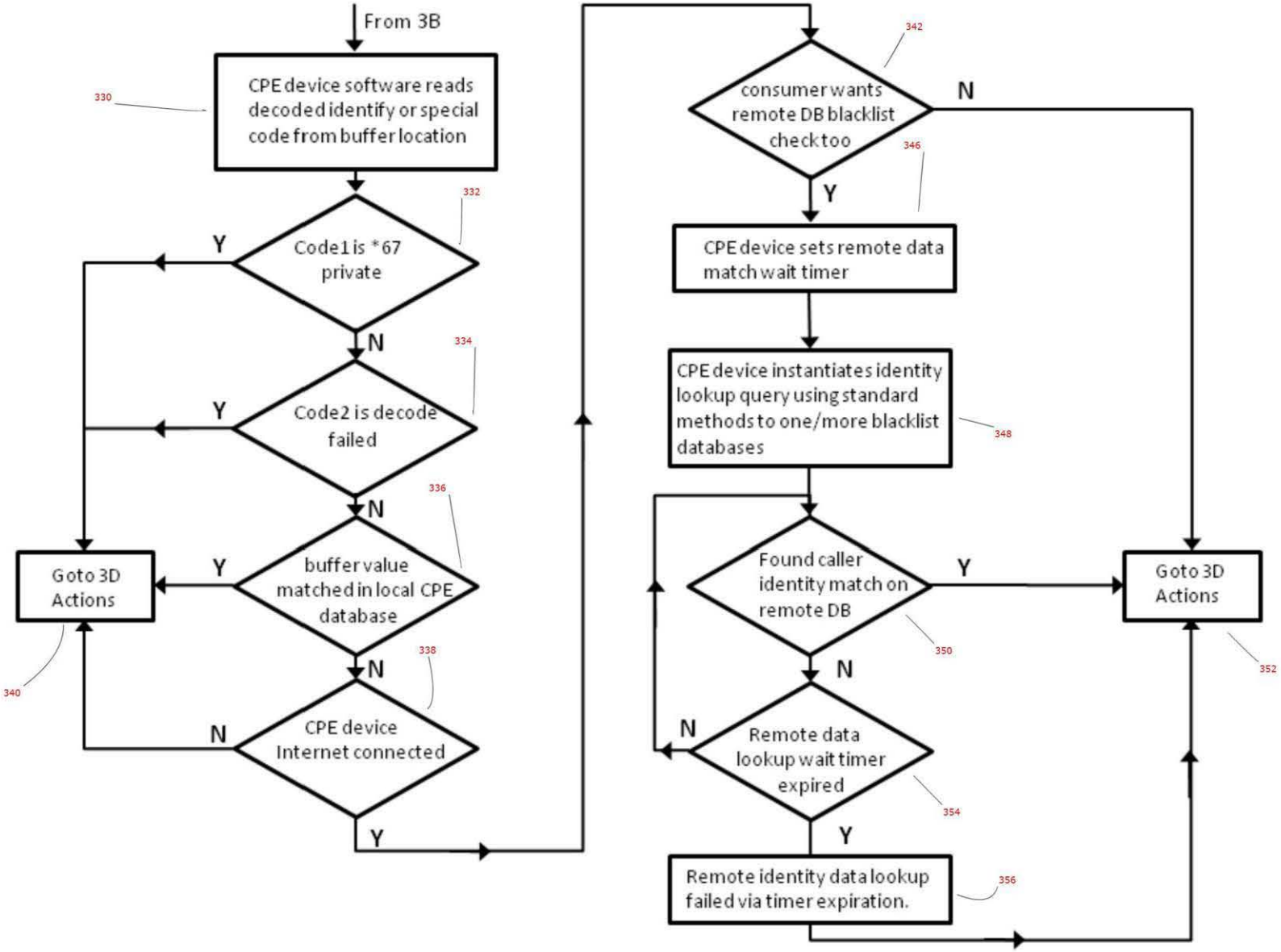

FIG. 3C

FIG.3D

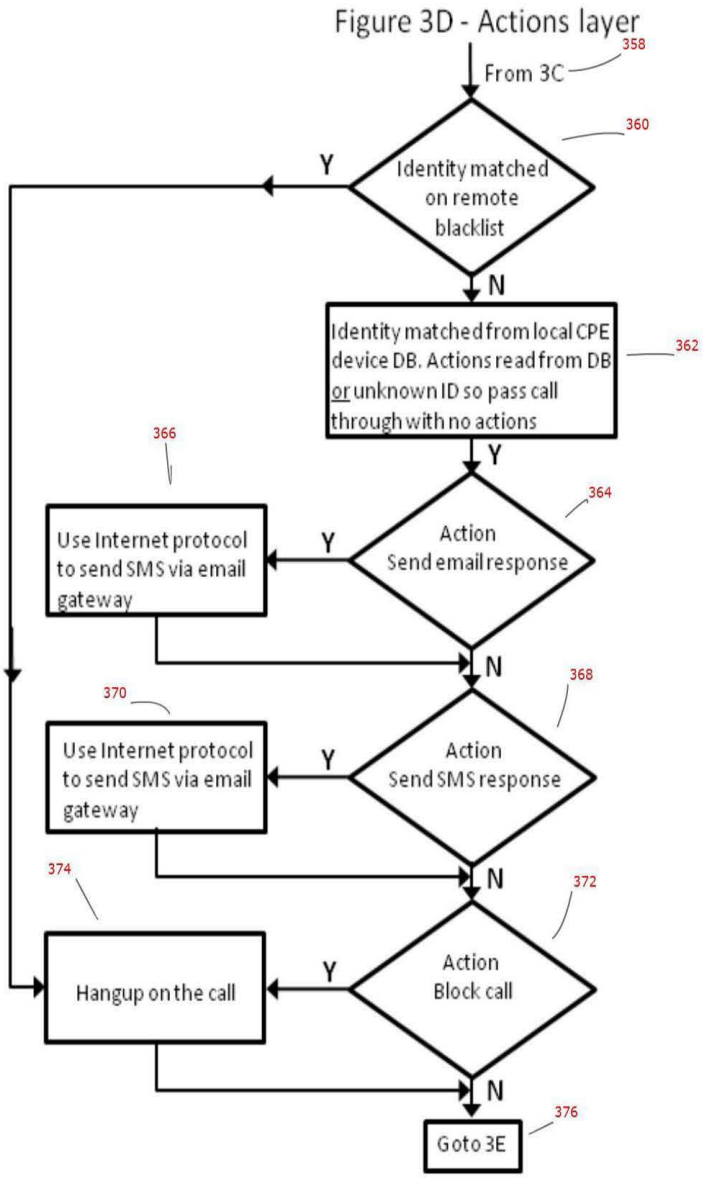
Figure 3D - Actions layer
From 3C
358
Identity matched on remote blacklist
360
Y
N
Identity matched from local CPE device DB. Actions read from DB or unknown ID so pass call through with no actions
362
Y
366
Use Internet protocol to send SMS via email gateway
Y
Action Send email response
364
N
370
Use Internet protocol to send SMS via email gateway
Y
Action Send SMS response
368
N
374
Hangup on the call
Y
Action Block call
372
N
Goto 3E
376

Figure 3E – Logging and data aggregation layer

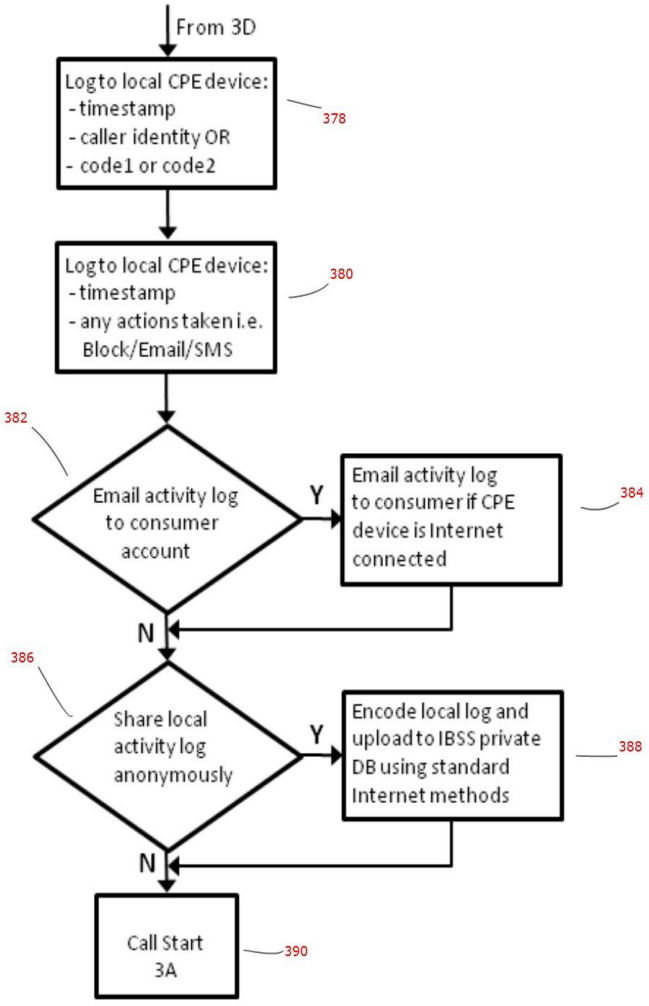

FIG. 3E

Figure 4 – Internet Based Servers and Service (IBSS)databases

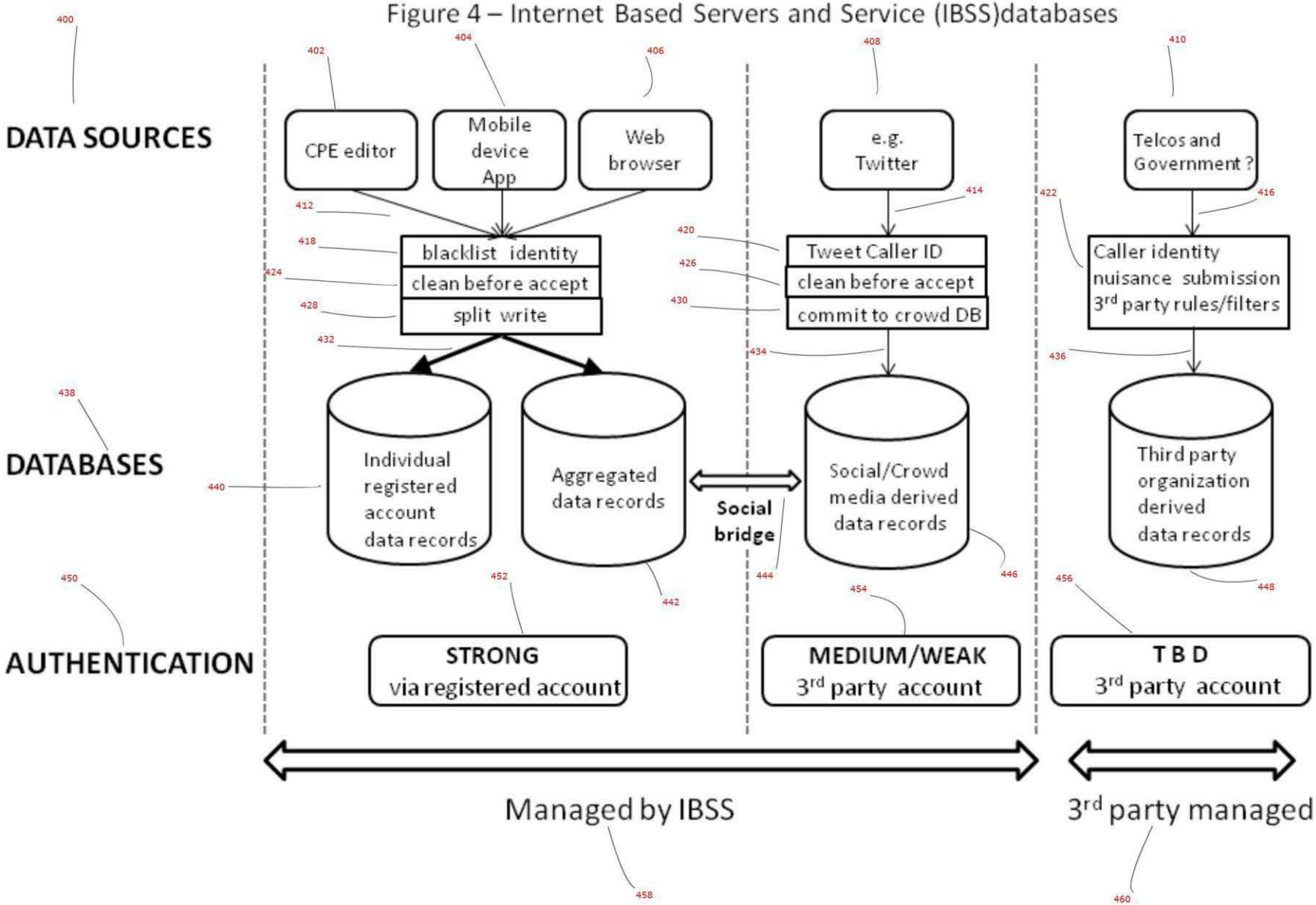

FIG. 4

Figure 5 –Client software editor

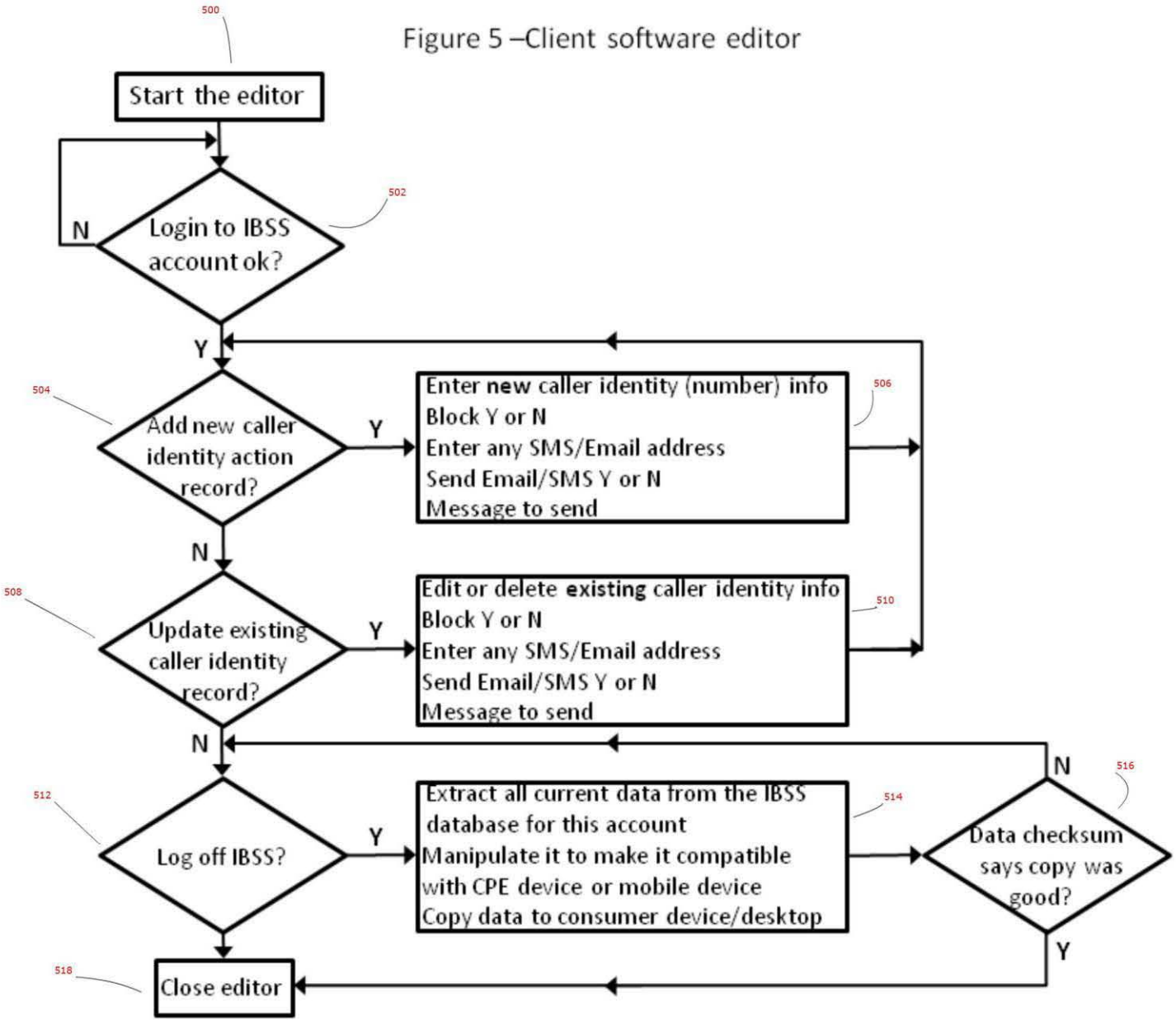

FIG. 5

Figure 6 – Updating mechanisms for CPE and mobile device local database(s)

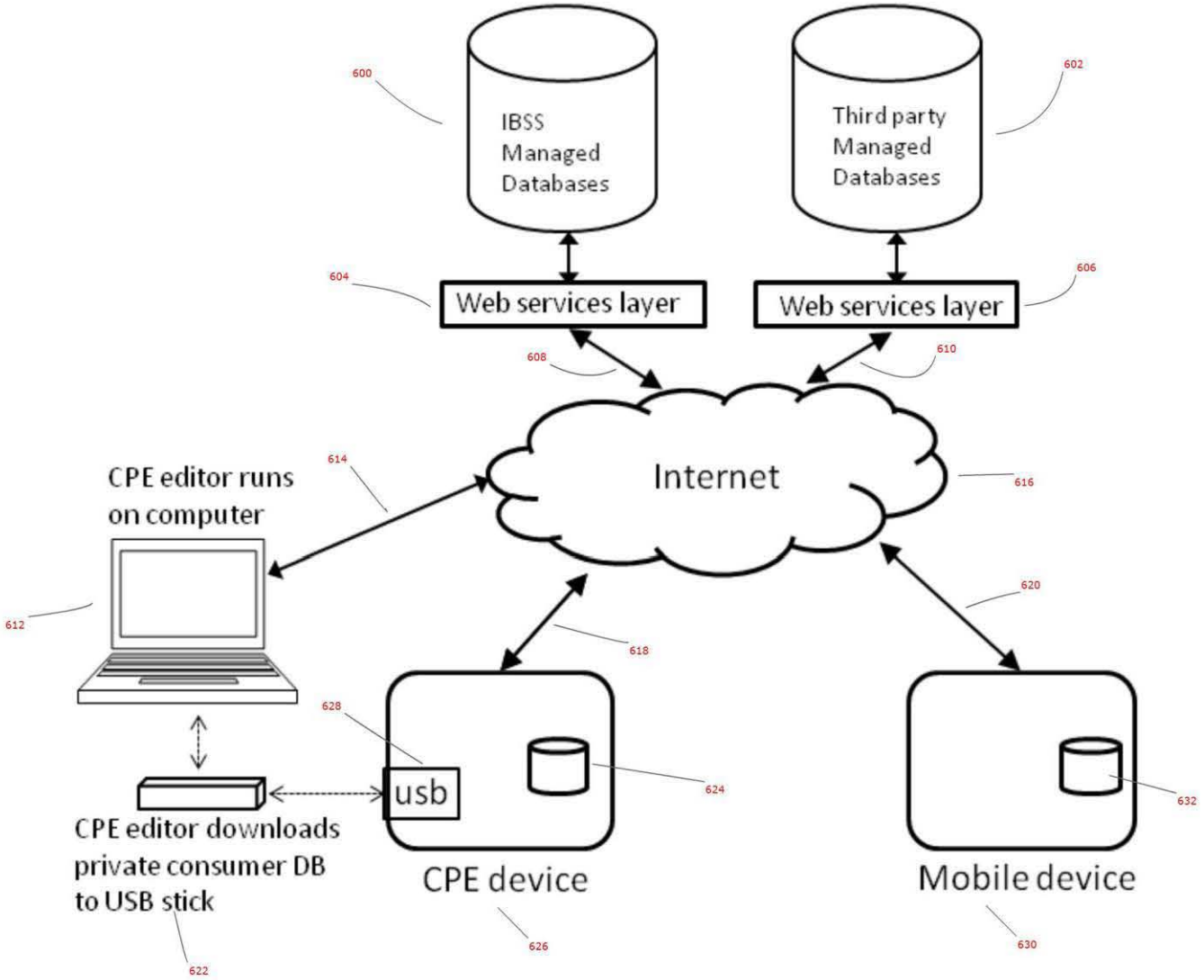

FIG. 6