US 20120042005A1

(19) **United States**

(12) **Patent Application Publication**

Papakostas et al.

(10) **Pub. No.: US 2012/0042005 A1**

(43) **Pub. Date: Feb. 16, 2012**

(54) **SYSTEMS, METHODS, AND APPARATUS TO MONITOR MOBILE INTERNET ACTIVITY**

(76) Inventors: **Achilleas Papakostas**, Richardson, TX (US); **Michael Andrew Yonker**, Dallas, TX (US)

(21) Appl. No.: **12/856,651**

(22) Filed: **Aug. 14, 2010**

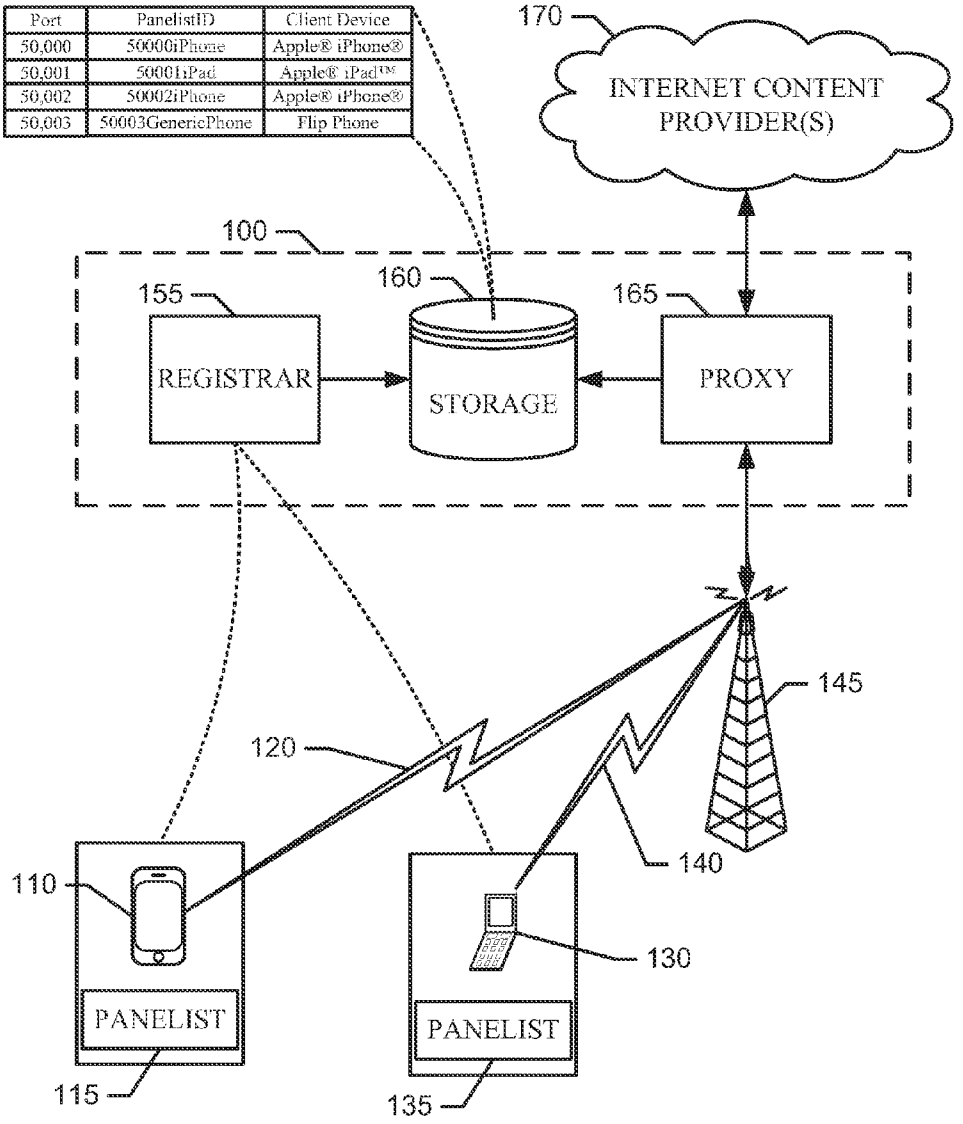
Publication Classification

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/203**; 709/217

(57) **ABSTRACT**

Systems, methods, and apparatus to monitor mobile Internet activity are disclosed. An example method comprises receiving a request for Internet content on a port of a proxy, the request originating from a mobile device transmitting requests via a cellular wireless access point; associating the request for Internet content with a mobile device based on the first port; requesting content from an Internet content provider identified in the request for Internet content, the Internet content provider being different than the proxy; and transmitting the content.



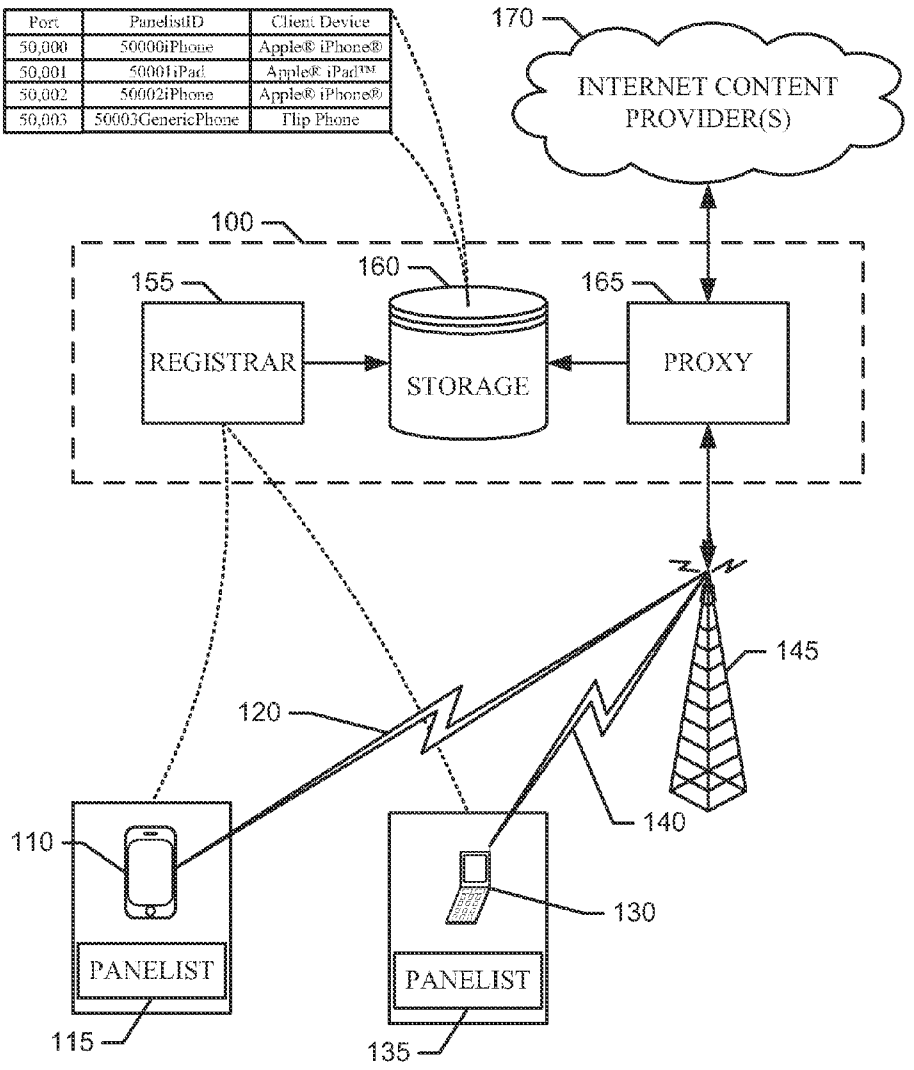

Port
PanelistID
Client Device
50,000
50000iPhone
Apple® iPhone®
50,001
50001iPad
Apple® iPad™
50,002
50002iPhone
Apple® iPhone®
50,003
50003GenericPhone
Flip Phone
170
INTERNET CONTENT PROVIDER(S)
100
155
REGISTRAR
160
STORAGE
165
PROXY
145
120
140
110
PANELIST
115
130
PANELIST
135

FIG. 1

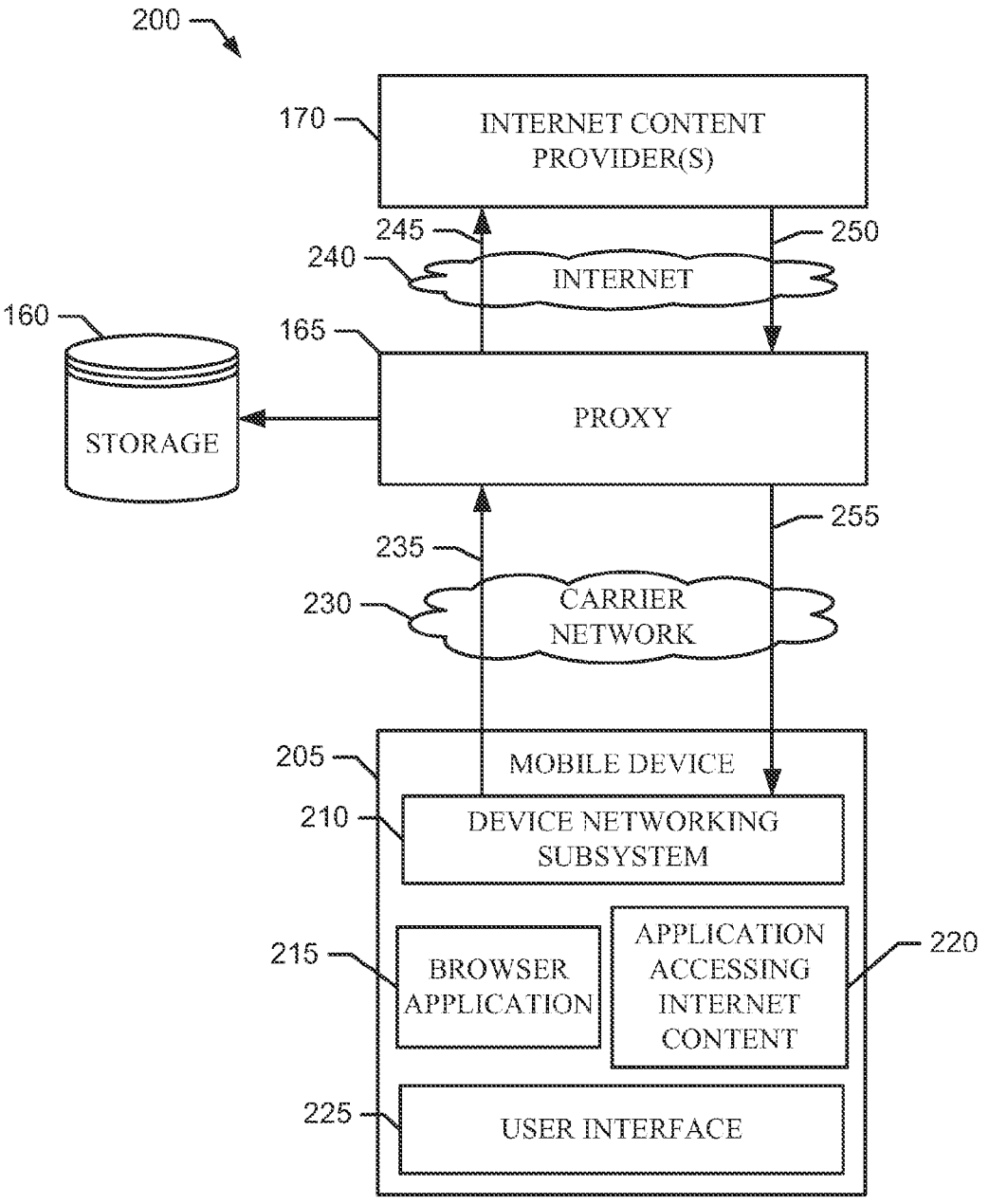

200
170
INTERNET CONTENT PROVIDER(S)
245
250
240
INTERNET
160
165
STORAGE
PROXY
255
235
230
CARRIER NETWORK
205
MOBILE DEVICE
210
DEVICE NETWORKING SUBSYSTEM
215
BROWSER APPLICATION
APPLICATION ACCESSING INTERNET CONTENT
220
225
USER INTERFACE

FIG. 2

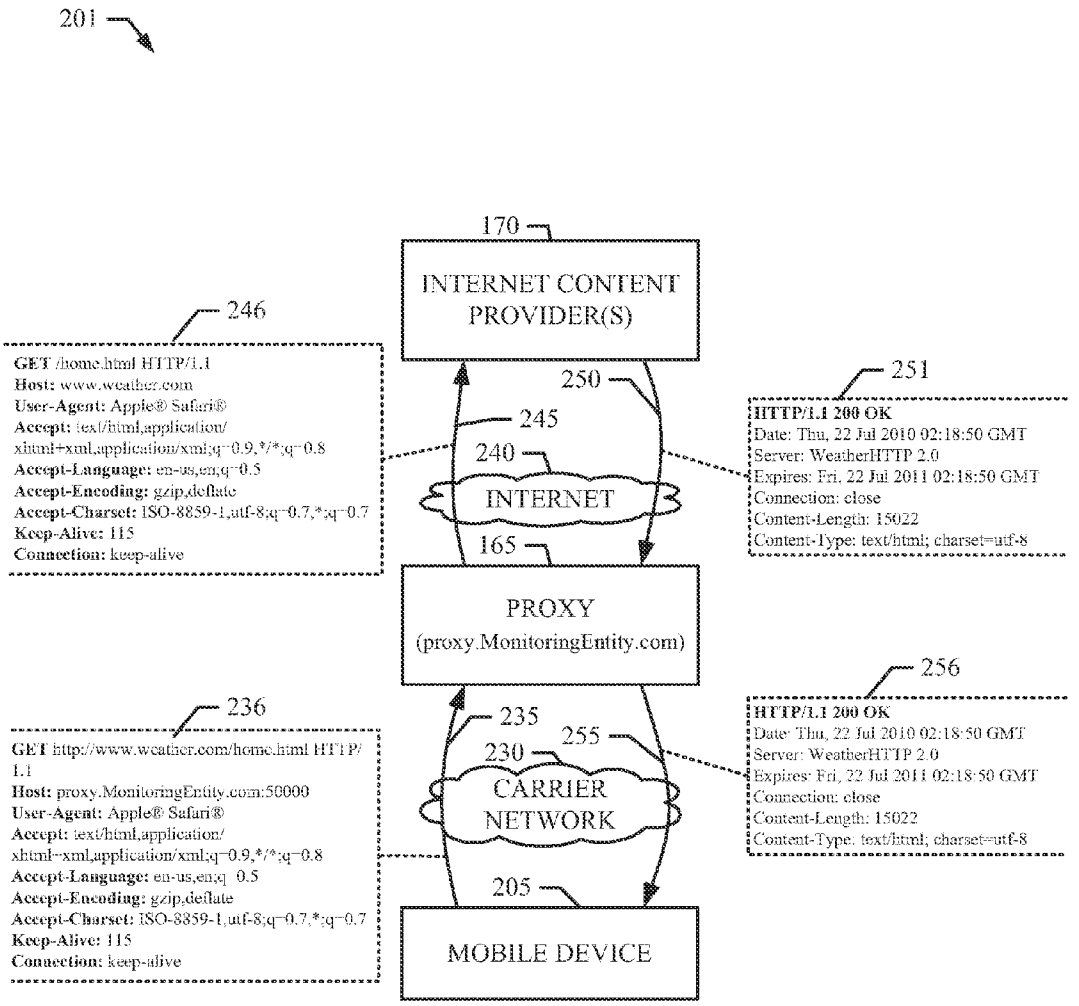
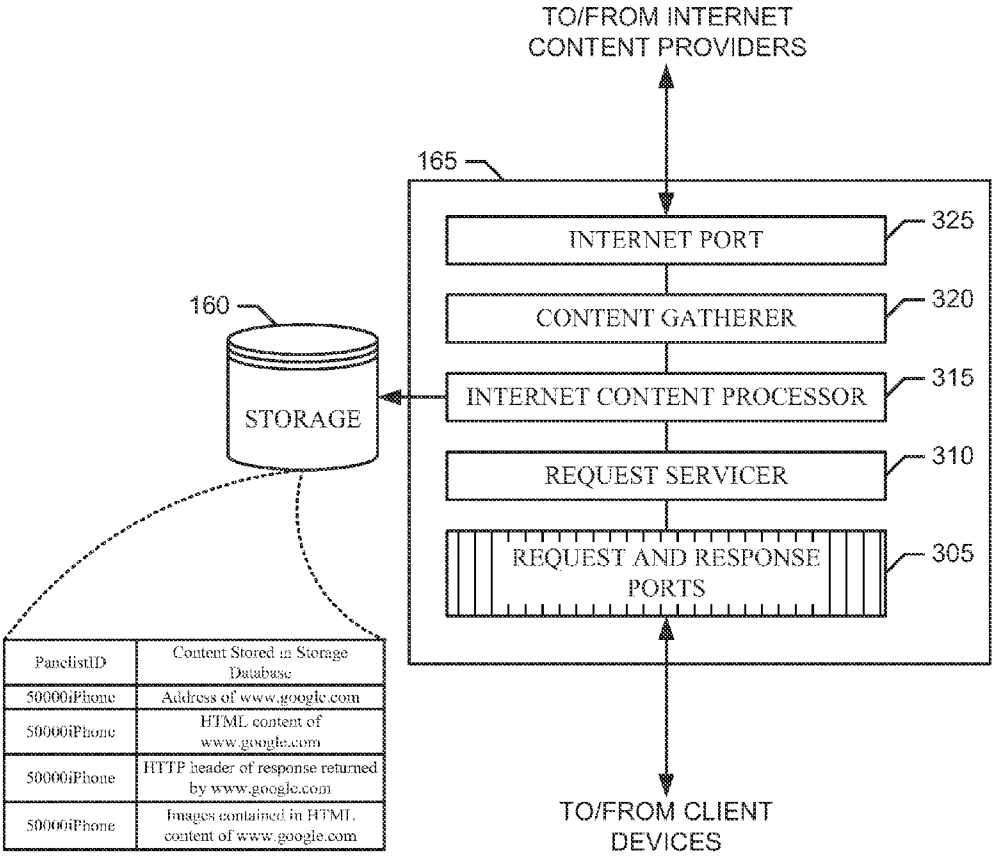

201
170
INTERNET CONTENT PROVIDER(S)
246
GET /home.html HTTP/1.1
Host: www.weather.com
User-Agent: Apple® Safari®
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
250
245
240
INTERNET
165
251
HTTP/1.1 200 OK
Date: Thu, 22 Jul 2010 02:18:50 GMT
Server: WeatherHTTP 2.0
Expires: Fri, 22 Jul 2011 02:18:50 GMT
Connection: close
Content-Length: 15022
Content-Type: text/html; charset=utf-8
PROXY
(proxy.MonitoringEntity.com)
236
GET http://www.weather.com/home.html HTTP/1.1
Host: proxy.MonitoringEntity.com:50000
User-Agent: Apple® Safari®
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
235
230
255
CARRIER NETWORK
256
HTTP/1.1 200 OK
Date: Thu, 22 Jul 2010 02:18:50 GMT
Server: WeatherHTTP 2.0
Expires: Fri, 22 Jul 2011 02:18:50 GMT
Connection: close
Content-Length: 15022
Content-Type: text/html; charset=utf-8
205
MOBILE DEVICE

FIG. 2A



PanelistID	Content Stored in Storage Database
50000iPhone	Address of www.google.com
50000iPhone	HTML content of www.google.com
50000iPhone	HTTP header of response returned by www.google.com
50000iPhone	Images contained in HTML content of www.google.com

Port	Content Stored in Storage Database
50000	Address of www.google.com
50000	HTML content of www.google.com
50000	HTTP header of response returned by www.google.com
50000	Images contained in HTML content of www.google.com

FIG. 3

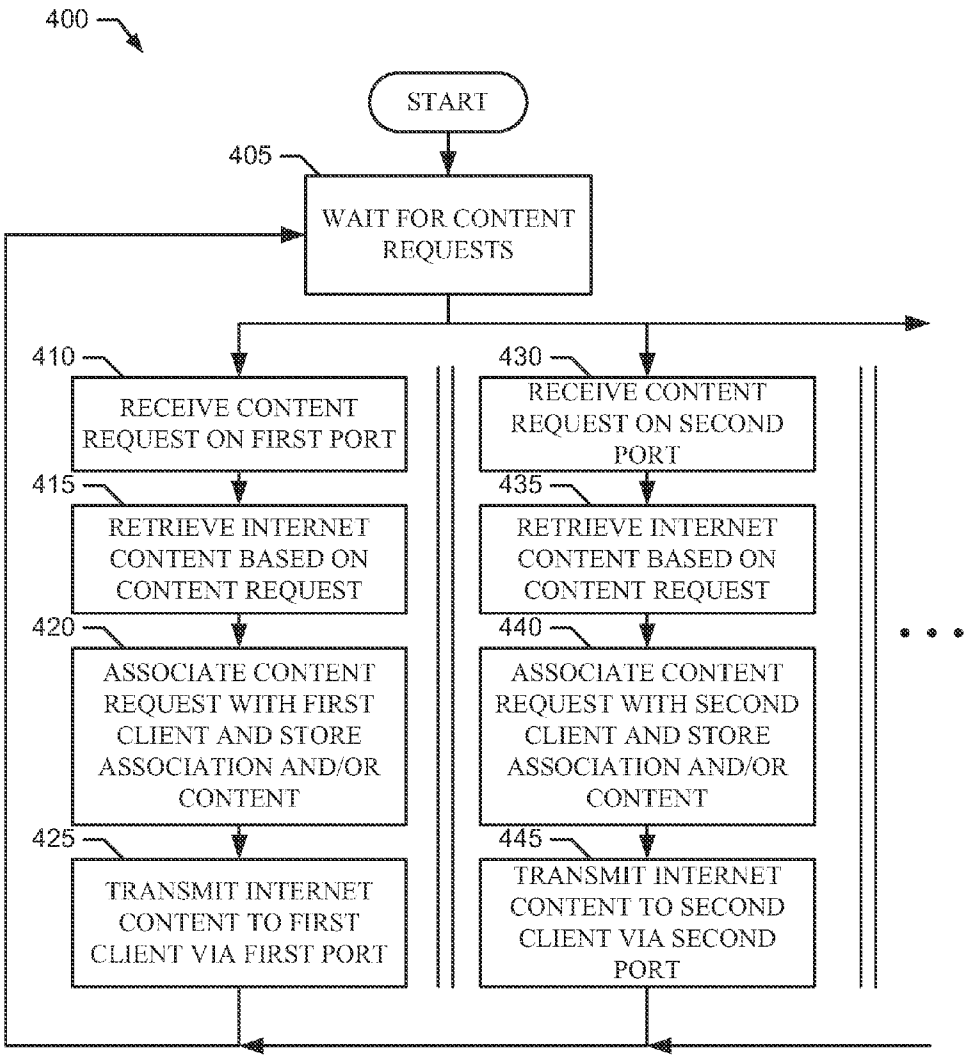

400
START
405
WAIT FOR CONTENT REQUESTS
410
RECEIVE CONTENT REQUEST ON FIRST PORT
415
RETRIEVE INTERNET CONTENT BASED ON CONTENT REQUEST
420
ASSOCIATE CONTENT REQUEST WITH FIRST CLIENT AND STORE ASSOCIATION AND/OR CONTENT
425
TRANSMIT INTERNET CONTENT TO FIRST CLIENT VIA FIRST PORT
430
RECEIVE CONTENT REQUEST ON SECOND PORT
435
RETRIEVE INTERNET CONTENT BASED ON CONTENT REQUEST
440
ASSOCIATE CONTENT REQUEST WITH SECOND CLIENT AND STORE ASSOCIATION AND/OR CONTENT
445
TRANSMIT INTERNET CONTENT TO SECOND CLIENT VIA SECOND PORT

FIG. 4

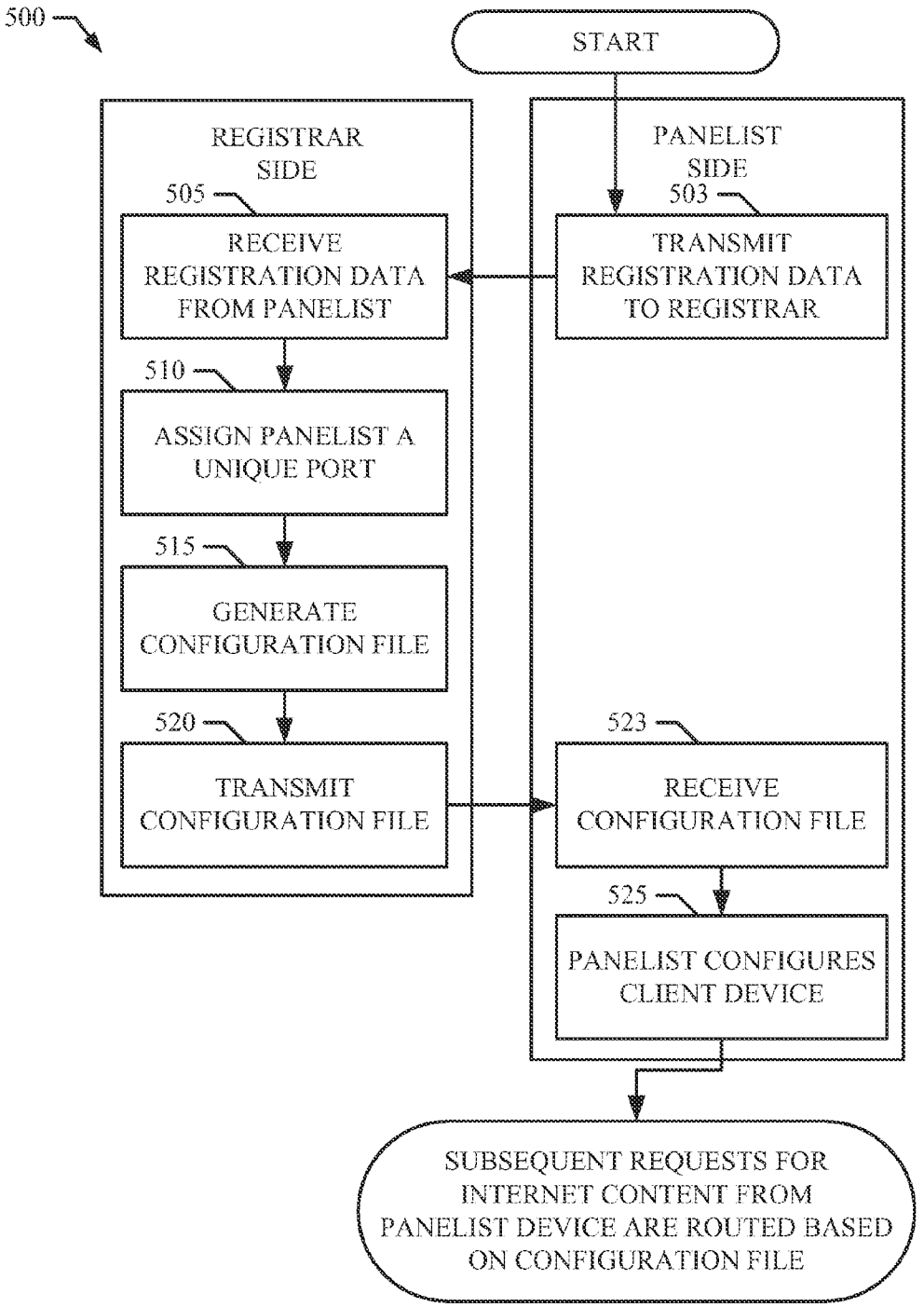

500
START
REGISTRAR SIDE
PANELIST SIDE
505
RECEIVE REGISTRATION DATA FROM PANELIST
503
TRANSMIT REGISTRATION DATA TO REGISTRAR
510
ASSIGN PANELIST A UNIQUE PORT
515
GENERATE CONFIGURATION FILE
520
TRANSMIT CONFIGURATION FILE
523
RECEIVE CONFIGURATION FILE
525
PANELIST CONFIGURES CLIENT DEVICE
SUBSEQUENT REQUESTS FOR INTERNET CONTENT FROM PANELIST DEVICE ARE ROUTED BASED ON CONFIGURATION FILE

FIG. 5

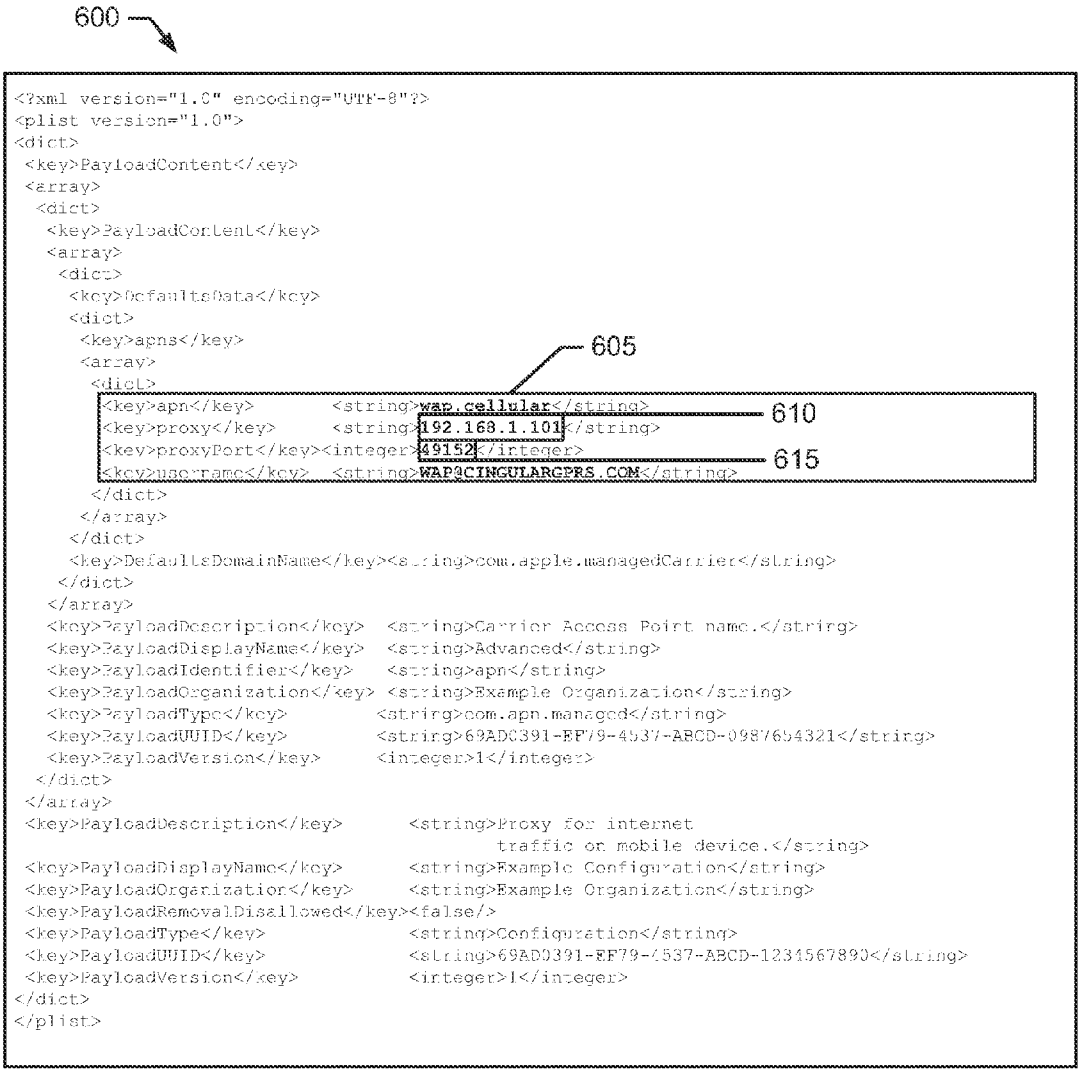

600
605
610
615
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>DefaultsData</key>
<dict>
<key>apns</key>
<array>
<dict>
<key>apn</key> <string>wap.cellular</string>
<key>proxy</key> <string>192.168.1.101</string>
<key>proxyPort</key><integer>49152</integer>
<key>username</key> <string>WAP@CINGULARGPRS.COM</string>
</dict>
</array>
</dict>
<key>DefaultsDomainName</key><string>com.apple.managedCarrier</string>
</dict>
</array>
<key>PayloadDescription</key> <string>Carrier Access Point name.</string>
<key>PayloadDisplayName</key> <string>Advanced</string>
<key>PayloadIdentifier</key> <string>apn</string>
<key>PayloadOrganization</key> <string>Example Organization</string>
<key>PayloadType</key> <string>com.apn.managed</string>
<key>PayloadUUID</key> <string>69ADC391-EF79-4537-ABCD-098765432l</string>
<key>PayloadVersion</key> <integer>1</integer>
</dict>
</array>
<key>PayloadDescription</key> <string>Proxy for internet
traffic on mobile device.</string>
<key>PayloadDisplayName</key> <string>Example Configuration</string>
<key>PayloadOrganization</key> <string>Example Organization</string>
<key>PayloadRemovalDisallowed</key><false/>
<key>PayloadType</key> <string>Configuration</string>
<key>PayloadUUID</key> <string>69AD0391-EF79-4537-ABCD-1231567890</string>
<key>PayloadVersion</key> <integer>1</integer>
</dict>
</plist>

FIG. 6

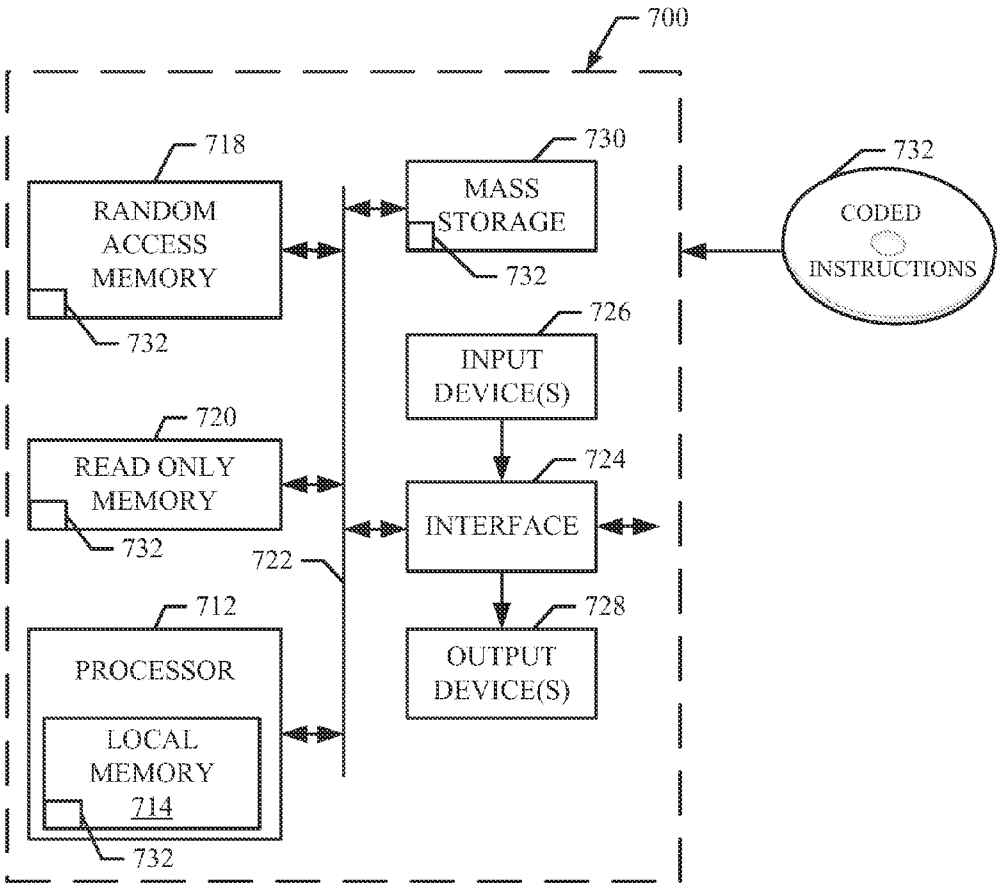

700
718
RANDOM ACCESS MEMORY
732
730
MASS STORAGE
732
732
CODED INSTRUCTIONS
726
INPUT DEVICE(S)
720
READ ONLY MEMORY
732
724
INTERFACE
722
712
PROCESSOR
LOCAL MEMORY 714
732
728
OUTPUT DEVICE(S)

FIG. 7

SYSTEMS, METHODS, AND APPARATUS TO MONITOR MOBILE INTERNET ACTIVITY

FIELD OF THE DISCLOSURE

[0001] This disclosure relates generally to monitoring Internet activity, and, more particularly, to systems, methods, and apparatus to monitor mobile Internet activity.

BACKGROUND

[0002] In recent years, methods of accessing Internet content have evolved. For example, Internet content was formerly primarily accessed via computer systems such as desktop and laptop computers. Recently, handheld mobile devices (e.g., smartphones) have been introduced that allow users to request and view Internet content. Typically, but not always, mobile devices request and receive Internet content via a wireless access network such as a cellular network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] FIG. **1** is a block diagram of an example system to monitor mobile Internet activity.

[0004] FIGS. **2** and **2**A are a block diagrams illustrating an example request and response flow through the example system of FIG. **1**.

[0005] FIG. **3** is a block diagram of the example proxy of FIG. **1**.

[0006] FIG. **4** is a flowchart representative of example machine-readable instructions that may be executed to implement the example proxy of FIGS. **1**, **2**, and **3**.

[0007] FIG. **5** is a flowchart representative of example machine-readable instructions that may be executed to implement the example registrar of FIG. **1**.

[0008] FIG. **6** illustrates an example configuration file that may be generated by the example registrar of FIG. **1**.

[0009] FIG. **7** is a block diagram of an example computer that may execute, for example, the machine-readable instructions of FIGS. **4** and/or **5** to implement the example monitor of FIGS. **1**, **2**, and **3**, and/or the example registrar of FIG. **1**.

DETAILED DESCRIPTION

[0010] Mobile monitoring companies desire to gain knowledge on how users interact with their handheld mobile devices such as smartphones. In particular, the mobile monitoring companies want to monitor Internet traffic to and/or from the handheld mobile devices to, among other things, monitor exposure to advertisements, determine advertisement effectiveness, determine user behavior, identify purchasing behavior associated with various demographics, etc. Some known systems have utilized a proxy server to monitor Internet content being transmitted to and from the monitored device.

[0011] Such known monitoring systems implemented the proxy server as an HTTP proxy that communicated with monitored handheld devices via a single port and required the monitored devices to provide authentication credentials including a username/device name and password that uniquely identified the mobile device involved in this Internet communication. These monitoring systems allowed mobile monitoring companies to associate Internet activity with the mobile device it originated from based on the username and password. Internet activity on handheld mobile devices is not limited to use of browsers (e.g., Apple® Safari®). For example, the Apple® iPhone® and the Apple® iPad™ support many third party applications (sometimes referred to as "Apps") accessing Internet content to perform a special function. For example, a weather application may request and display HTTP data from www.weather.com. These apps typically do not permit unrestricted browsing from website to website on the Internet (although they may permit movement within a defined set of webpages). Thus, apps typically provide access to a limited set of data on the Internet. In contrast, a browser enables a user to access virtually any publicly available site on the Internet (subject to restrictions such as content blockers) and directly shows the user the contents a website such as www.weather.com.

[0012] While some applications accessing Internet content properly respond to proxy requests to provide credentials, many applications, such as the weather application from the previous example, do not presently support proxy authentication and therefore fail to function if a proxy requests credentials. This can be frustrating for panelists and may cause the panelist to abandon participation in the monitoring panel. Furthermore, it is desirable for monitoring entities to monitor Internet activity without affecting the manner in which users behave. Causing application failure due to a monitoring technique is inconsistent with that desire.

[0013] To avoid errors inherent in using an authenticated proxy, the example system shown in FIG. **1** employs an un-authenticated proxy. Use of a proxy that does not request authentication credentials (i.e., an un-authenticated proxy), is problematic in that such an approach does not lend itself to user identification, and user identification is necessary to correlate activity behavior with demographics. The example system of FIG. **1** addresses this problem by hosting a unique un-authenticated port for each panelist and/or mobile device and instructing each monitored mobile device to communicate using its uniquely assigned port. This use of multiple ports allows the monitoring entity to uniquely associate the Internet traffic it detects with the panelist and/or mobile device involved in such traffic. While previous monitoring systems hosted a proxy connection on a single port such as port **8080**, the proposed monitoring system hosts connections on many available ports (e.g., ports **0** to **65535**). Certain ports are omitted from the list of available ports if those ports are associated with other Internet services. For example, ports **0** through **1023** are defined as Well Known Ports by the Internet Assigned Numbers Authority (IANA), and are prohibited from use without registration. Thus, Well Known Ports are not used in the example system of FIG. **1**.

[0014] The example monitoring system of FIG. **1** records the identifications of data that the client devices request and/or receive and/or some or all of the data itself. Identifications of data and/or the data itself (e.g., web content) is collectively referred to herein as "session data." The session data is recorded in association with the panelist via the port number on which the session data is transmitted. From the recorded session data and the port number, the monitoring system can uniquely identify the site(s) that a particular panelist is visiting and how the panelist interacted with their mobile device, while avoiding interruption of services for the panelist.

[0015] FIG. **1** is a block diagram of an example system **100** to monitor mobile Internet activity. The example system monitors Internet traffic to and/or from handheld mobile devices (e.g., a first client device **110** associated with a first panelist **115**, a second client device **130** associated with a second panelist **135**). The monitored Internet traffic between the monitored devices (e.g., the client device **110**, and the

client device **130**) and Internet sites (illustrating Internet content provider(s) **170**) is routed to the example monitoring system **100**. As shown in FIG. **1**, the traffic passes through a wireless (e.g., cellular) communication system (e.g., an Internet service provider **145** and communicative links **120**, **140**). The example monitoring system **100** includes a registrar **155**, a storage database **160**, and a proxy **165**.

[0016] The example first and second client devices **110**, **130** of FIG. **1** are handheld mobile devices. While in the illustrated example the first client device **110** is shown as an Apple® iPhone® and the second client device **130** is shown as a flip phone, any other type of device may be used. For example, other types or phones, a laptop computer, a desktop computer, a personal digital assistant (PDA), a netbook, or a tablet computer (e.g., an Apple® iPad™) may additionally or alternatively be used. The first and second client devices **110**, **130** may implement any mobile operating system, and may implement any type of hardware and/or form factor. In the illustrated example, the first and second client devices **110**, **130** are mobile devices and communicate via the first and second wireless communication links **120**, **140**.

[0017] The first and second communication links **120**, **140** of the illustrated example are cellular communication links. However, any other method and/or system of communication may additionally or alternatively be used such as, for example, an Ethernet connection, a Bluetooth connection, a WiFi connection, etc. Further, the example first and second communication links **120**, **140** of FIG. **1** implement a cellular connection via a Global System for Mobile Communications (GSM). However, any other systems and/or protocols for communications may be used such as, for example, Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Worldwide Interoperability for Microwave Access (WiMAX), Long Term Evolution (LTE), etc. When alternative communication methods and/or systems are used (e.g., WiFi), the topology of the communication system may include a firewall that blocks Internet communications using certain ports. When the port uniquely assigned to a panelist is blocked by the firewall, the client device may fail to operate as expected and/or present error messages to the panelist.

[0018] The first and second panelists **115**, **135** of the illustrated example are panelists participating in a monitoring service. Although the example system of FIG. **1** is a panelist-based system, non-panelist and/or hybrid panelist systems may alternatively be employed. In the panelist system of the illustrated example, demographic information is obtained from the user when the user joins and/or registers for the panel. The demographic information may be obtained from the user via a telephone interview, by having the user complete an online survey, etc. Additionally or alternatively, panelists may be contacted and/or enlisted using any desired methodology (e.g., random selection, statistical selection, phone solicitations, Internet advertisements, surveys, advertisements in shopping malls, etc.).

[0019] In the illustrated example, the first and second panelists **115**, **135** are associated with the first and second client devices **110**, **130**, respectively. In the illustrated example, the client devices **110**, **130** are owned, leased, or otherwise belong to their respective panelists. The monitoring entity of the illustrated example does not provide the client devices. In other systems, panelists may be provided with client devices to participate in the panel. While in the illustrated example, the first and second client devices **110**, **130** are each associated with a single panelist, the first and second client devices **110**, **130** may alternatively be associated with more than one panelist. For example, a family may have a single client device that may be shared amongst multiple users. The sharing of a client device is less common when the client device is a cellular phone than when the client device is a portable computer (e.g., an Apple® iPad™).

[0020] The Internet service provider **145** of the illustrated example provides wireless Internet service to the first and second client devices **110**, **130** via the communication links **120**, **140**. In the illustrated example, the wireless service is provided via a cellular connection. However, the Internet service provider **145** may provide Internet service via any other type of connection. Further, the Internet service provider **145** may implement the cellular connection via a Global System for Mobile Communications (GSM). However, any other systems and/or protocols for communications may be used. In practice, the Internet service provider **145** is sometimes referred to as a carrier, and provides a access to carrier network to the client devices.

[0021] In the illustrated example, the monitoring system **100** is shown as multiple computing systems. However, the monitoring system **100** may ultimately be comprised of a single computing system. In the illustrated example, the monitoring system **100** includes the registrar **155**, the storage database **160**, and the proxy **165**. However, additional structures may be implemented to carry out one or more portions of the functionalities implemented by the registrar **155**, the storage database **160**, and/or the proxy **165**, and/or other functions.

[0022] In the example of FIG. **1**, the registrar **155** receives registration information from the panelists **115**, **135** and stores a record identifying the panelist **115**, **135** and/or their respective client devices **110**, **130**. In the illustrated example, the record identifying the panelist **115**, **135** is the port number assigned to the panelist (e.g., the port assigned to the panelist may be 50,000 and the record identifying the panelist may be 50,000). In the illustrated example, the received registration information includes demographic information. However, any other information may additionally or alternatively be collected. The registration information may include, for example, information identifying the model of mobile device associated with the panelist, a mailing address associated with the panelist, an email address associated with the panelist, a phone number associated with the mobile device, a unique identifier of the panelist and/or mobile device (e.g., a social security number of the panelist, a phone number of the mobile device, a zip code of the panelist, and/or any combination or derivation of any information related to the panelist and/or mobile device), the age of the panelist, the gender of the panelist, the race of the panelist, the marital status of the panelist, the income of the panelist and/or the household of the panelist, the employment status of the panelist, where the panelist typically intend to use their device, how long the panelist has owned their device, the education level of the panelist and/or any other information related to the panelist or the mobile device.

[0023] In the illustrated example, the registration data is received by the registrar **155** via an electronic interface (e.g., by a panelist entering data into a form at a website or answering survey questions at a website). However, the registrar may receive the registration data may via other means. For example, the registrar may receive the registration data via a personal interview (by telephone or in person), a telephone interface, direct mailing, purchased lists, etc. While the reg-

istrar **155** of the illustrated example is an electronic system, the registrar **155** may alternatively be implemented manually by a person or group of people collecting and entering the registration data into the storage database **160**.

[0024] Upon receiving the registration data, the registrar **155** of the illustrated example creates a record associating the panelist and a device identifier information with the collected demographic information. The registrar **155** may also assign a unique alphanumeric identifier to the panelist or device. The identifier may be based on, for example, a serial number of the client device. The record is stored in the storage database **160**. In the illustrated example, the registrar **155** also assigns a unique port number to the panelist **115**, **135** and/or the client device **110**, **130** and stores the port number in the record (or in association with the record for that panelist and/or client device). As noted above, in addition to assigning and storing the port number, the registrar may assign and store additional identifiers. For example, the registrar may assign and store an identifier of the client device and/or the panelist. The panelist or client device identifier(s) may be the same as the port number, or they may be different from the port number.

[0025] In addition to assigning and storing the port number, the registrar **155** of the illustrated example generates a configuration document. In the illustrated example, the configuration document is an Extensible Markup Language (XML) file implementing a property list (referred to herein as a plist) file comprising configuration data such as the port number and an Internet proxy address to be used by the corresponding panelist and/or client device. However, any other type of document may be generated such as, for example, a comma separated (CSV) document, a Portable Document Format (PDF) document, a Microsoft® Word® document, etc. In the illustrated example, the configuration document is signed using a public/private key infrastructure. For example, the configuration document may be signed via a digital certificate. However, the configuration may alternatively not be signed. If the configuration document is not signed, it may appear as an invalid configuration file to the panelist, which may cause the panelist to abandon participation in the panel. The configuration file is sent to the corresponding client device (e.g., via an email message with the file attached or with a link to the file). The client device then interprets the data in the configuration file, thereby applying the data (e.g., the port number and Internet proxy address) to future communication of the mobile device. In the illustrated example the configuration file causes the mobile device to send all Internet traffic to the Internet address of the proxy **165** and to specify the unique port number assigned to the client device in such communication. As a result, all Internet communications to and/or from the mobile device are addressed to a uniquely assigned port of the proxy **165** and can, thus, be identified or associated with that particular client device. In the illustrated example the plist file is implemented for interpretation by an Apple® iPhone® and/or an Apple® iPad™. However, the mobile device may be any other type of mobile device. Further, the configuration file may be custom generated for the particular type of mobile device based on the model of the mobile device identified to (or by) the registrar as part of the registration data.

[0026] While in the example of FIG. **1**, the document is an electronic document that may be interpreted by the client device to automatically configure the client device to communicate Internet related messages to a unique port of the proxy **165**, the document may additionally or alternatively comprise an instruction document that may guide the panelist on how to configure the client device to communicate with the proxy. The instruction document may thereby instruct the panelist on how to apply the configuration file or may instruct the panelist on how to directly apply the data stored in the configuration file to the client device.

[0027] As noted above, the registrar **155** transmits the configuration document to the panelist and/or client device. In the illustrated example, the configuration file is provided via an electronic mail (email) message. The email message includes a hyperlink to download the configuration file to the client device. However, any other methods of transmitting the configuration file may additionally or alternatively be used. For example, the configuration file may be transmitted as an attachment to the email message, the registrar **155** may transmit a short message service (SMS) message comprising a link to or a textural representation of an Internet address where the client device may download the configuration file, a direct mailing may be sent to the panelist comprising the instruction document and/or additionally comprising an electronic medium containing the configuration file, a telephone call may be placed to orally instruct the panelist on how to configure the client device, etc.

[0028] The registrar **155** of FIG. **1** is implemented by a processor executing instructions, but it could alternatively be implemented by an ASIC, DSP, FPGA, or other circuitry. The storage database **160** receives and stores identifiers associating the panelists **115**, **135** with the client devices **110**, **130** from the registrar **155**. Additionally, the storage database **160** receives and stores monitoring data from the proxy **165**. The monitoring data is associated with the corresponding panelist and/or client device via the port number used for the corresponding monitored Internet traffic. The storage database **160** may also be capable of storing data that is not identifiers and/or measurement data. For example, updated software and/or updated firmware for any component of the monitoring system **100** may be stored in the storage database **160**. Further, the storage database **160** may be capable of storing information that enables the registrar **155** to generate the configuration document. For example, the storage database **160** may store registration information such as the model of the client device **110**, **130**. Additionally, the storage database **160** may store demographic data as collected by the registrar **155**.

[0029] The storage database **160** may be any device for storing data such as, for example, flash memory, magnetic media, optical media, etc. Furthermore, the data stored in the storage database **160** may be in any data format such as, for example, binary data, comma delimited data, tab delimited data, structured query language (SQL) structures, etc. While in the illustrated example the storage database is illustrated as a single database, the storage database **160** may be implemented by multiple databases.

[0030] The proxy **165** of the illustrated example receives requests from the client devices **110**, **130** via the wireless Internet service provider **145**. The requests of the client devices **110**, **130** are received by the proxy **165** due to the configuration file having been applied to respective ones of the client device instructing the client device to transmit all subsequent requests through the proxy **165**. The proxy **165** is located at the Internet proxy address identified in the configuration file, and receives request via ports associated with client devices. In the illustrated example, the ports are Dynamic and/or Private Ports as defined by the Internet

Assigned Numbers Authority (IANA). Therefore, the range of assignable ports used by the illustrated proxy **165** for Internet traffic with monitored client devices is 49152 through 65535. By only using Dynamic and/or Private Ports, the group of panelists served by a single proxy **165** is effectively limited to 16383 client devices. This size can be expanded by using additional proxies at other Internet addresses. The additional proxies at other Internet addresses may be implemented by the same proxy **165** or by multiple proxies. For example, the proxy **165** may have multiple Internet addresses assigned to a network interface of the proxy **165** (e.g., virtual interfaces), or the proxy **165** may have multiple network interfaces each having an Internet address. While in the illustrated example only ports used within the Dynamic and/or Private Ports range are used, any other ports may additionally or alternatively be used. For example, ports within the Registered Ports range and/or the Well Known Ports range may potentially be used to increase the group of panelists to as large as 65535 panelists with a single proxy. In a scenario where a panel monitoring system such as the monitoring system **100** is being tested, a typically a panel will include at least sixty panelists and, thus, the proxy **165** will use at least sixty ports (e.g., one for each panelist). In a scenario where an ongoing panel is used, a panel size of at least 1,500 panelists may be used and, thus, the proxy **165** will use at least 1,500 ports (e.g., one for each panelist).

[0031] Upon receiving a request from a client device **110**, **130**, the proxy **165** retrieves the requested Internet content from the Internet content providers **170** (or from a local cache if, for example, it had previously been requested and stored). In order to identify the panelist associated with the request, communication to and from each specific panelist occurs over the uniquely assigned (e.g., dedicated) port. While the communication between a client device **110**, **130** use the proxy **165** occurs over a single port (e.g., the port assigned to that client device **110**, **130** by the registrar **155**), communication between the proxy **165** and the Internet content providers **170** may be implemented over any port. Typically, the port used by the proxy to communicate with content providers **170** is limited to hypertext transfer protocol (HTTP) data that occurs over port **80**. After retrieving the requested Internet content from the Internet content provider(s) **170**, in the illustrated example the content is relayed to the requesting client device **110**, **130** via the assigned port. Additionally or alternatively, the content may be relayed to the requesting client device **110**, **130** via a port other than the assigned port (e.g., port **80**).

[0032] The proxy **165** of the illustrated example stores the requests for Internet content and/or portion(s) of such requests originating from the client devices **110**, **130** in the storage database **160** in association with the port numbers over which the request was received. In storing the requests, the proxy **165** may additionally store other identifiers such as, for example, the identifier of the client device **110**, **130**, and/or the identifier of the panelist **115**, **135**. Additionally or alternatively, the proxy **165** may store a portion of the Internet content in the storage database **160**. For example, the proxy **165** may store the body of a webpage transmitted to the client device **110**, **130**. In another example, the proxy **165** may store an identifier of an advertisement appearing on the webpage transmitted to the client. This is particularly useful in situations where advertisements are rotated at websites. Additionally or alternatively, the proxy **165** may store characteristics of the response, such as, for example the HTTP header, a status code of the HTTP header, a content type of the HTTP header, etc.

[0033] The Internet content providers **170** supply content to clients via the Internet. In the illustrated example, the proxy **165** acts as an intermediary for the client devices **110**, **130**, and, thus, is the client of the Internet content providers **170**. Internet content is often supplied over port **80**, as most Internet content is in the form of HTTP data. However, any other port may be used to supply Internet content. For example, file transfer protocol (FTP) data may be transmitted over port **21**, HTTP over Secure Socket Layer (SSL) may be transmitted over port **443**, etc.

[0034] The Internet content providers **170** can be any provider. For example, the Internet content providers **170** may comprise a web server hosting webpages formatted as Hypertext Markup Language (HTML) content. Alternatively, the Internet content provider **170** may be an application server providing application content to applications accessing Internet content. The application content may be formatted as HTML, XML, or may use any other protocol or port to return content to the requester. In some examples, the application data is implemented in a protocol specifically targeted for an application requesting Internet content (e.g., as the weather application described above).

[0035] FIG. **2** is a block diagram **200** illustrating an example request and response flow through the example system of FIG. **1**. The block diagram **200** of FIG. **2** illustrates communication between a mobile device **205**, a carrier network **230**, the proxy **165**, the storage database **160**, the Internet **240**, and the Internet content providers **170**. The mobile device **205** represents either of the client devices **110**, **130** and comprises a device networking subsystem **210**, a browser application **215**, an application accessing Internet content **220**, and a user interface **225**. Additionally, the block diagram illustrates a first request **235**, a second request **245**, a first response **250**, and a second response **255**.

[0036] The device networking subsystem **210** provides a framework for transmitting and receiving content. The device networking subsystem **210** may be implemented via an application processor, a software system that facilitates networked communication, a browser engine, a baseband processor that transmits network traffic, and/or any other system that provides a framework for transmitting and receiving content. In the illustrated example, the device networking subsystem is implemented by the networking libraries provided in the Apple® iPhone® operating system. However, any other libraries, systems, or programs may additionally or alternatively be used.

[0037] The browser application **215** and application accessing Internet content **220** are applications that are executed by a processor of the mobile device **205**. The browser application **215** requests HTTP Internet content from Internet content providers **170**, and renders the HTTP content for display. Additionally or alternatively, the browser application may request and render HTTPS Internet content. In some examples, the browser application is implemented by Apple® Safari®. However, any other application may alternatively be used. For example, Pocket Internet Explorer may be used. In some examples, the HTTP Internet content is HTML content. However, the content may be presented in any format that may be rendered by the browser application **215**.

[0038] The application accessing Internet content **220** may be any application on the mobile device that requests Internet content. For example, the application accessing Internet content **220** may be a weather application accessing Internet content provided by www.weather.com. The Internet content provider **170** providing content for www.weather.com may respond to content requests with HTML data. However, any other type of data may be contained in the content request. For example, the Internet content provider **170** providing content for www.weather.com may provide an XML file containing a condensed weather forecast. Additionally or alternatively, the application accessing Internet content **220** may request media such as, for example, photos, video, audio, etc. Typically, applications accessing Internet content **220** are limited to a small amount of information to be displayed. For example, the weather application may not be able to display sports news. Although the browser **215** or the application accessing Internet content **220** may initiate requests for content, in some devices, such as the Apple® iPhone®, requests are formatted and transmitted by the device networking subsystem **210** based on system wide settings that control routing and/or addressing of such requests (e.g., to a specific port of a proxy **165**).

[0039] The user interface **225** of the illustrated example provides a display to the user and receives input from the user. The user interface **225** may comprise hardware, a graphics library, and/or a graphics driver for displaying content to the panelist, and may comprise hardware, an input library, and/or an input driver for receiving input from the panelist. Either or both the browser application **215** and the application accessing Internet content **220** may utilize the user interface to display content and receive input.

[0040] The carrier network **230** is hosted by the Internet service provider **145**. In the illustrated example, the carrier network **230** is an Internet Protocol (IP) version 4 (IPv4) based network. However, any other networking technology may additionally or alternatively be implemented. For example, the carrier network may **230** implement the IP version 6 (IPv6) protocol. Further, the carrier network **230** of the illustrated example is implemented using communication links **120**, **140**. While cellular connections are shown, any other method of communication may additionally or alternatively be used such as, for example, an Ethernet network, a WiFi network, etc. Additionally, the carrier network **230** is shown as a public network. However, the network may be a private network.

[0041] The proxy **165** receives a first request **235** for Internet content from the mobile device, retrieves the content by sending a second request **245** to the corresponding content provider **170**, receive the content in a response **250** from the content provider **170**, and relays the content to the mobile device **205** via a second response **255**. In the illustrated example, the proxy **165** stores characteristics and/or identifiers of the request and/or response in the storage database **160**. These characteristics and/or identifiers may be, for example, a timestamp of the request and/or response, an IP address of the client, a user agent of the request, a status code of the response, a content type of the response, etc. However, the proxy **165** may additionally store the Internet content of the response in the storage database **160**. In relaying the request, the proxy **165** translates the port of the requests, as is described below in conjunction with FIG. **2**A.

[0042] The Internet **240** in the illustrated example is a public network. However, the a private network may instead be employed. For example, a network internal to an organization and/or company may be used to determine how members of the organization and/or employees of the company utilize internal web content via mobile devices.

[0043] The illustrated example shows, a communication stream for a single request. The first request **235** is transmitted to the proxy **165** from the mobile device **205** over the carrier network **230**. The first request **235** uses the unique port assigned to the mobile device **205** (e.g., port **50,000**), and is for HTTP content (e.g., the request is for content that is served over port **80**). However, the content requested may be requested over any port. For example, the request may be for file transfer protocol (FTP) content and may occur over port **21**. The proxy **165**, upon receiving the first request **235**, stores some or all of the request in the storage database **160**, and generates a second request **245**. The second request **245** is effectively a translation of the first address as shown in FIG. **2**A. The second request is addressed to the Internet content provider **170** identified in the first request **235**. The second request **245** in the illustrated example is transmitted via the Internet **240** over port **80**, as the first request **235** identified content to be served over port **80**. The Internet content provider **170** responds to the second request **245** with the first response **250**. The proxy **165** receives the first response **250** via port **80**, stores some or all of the request in the storage database **160**, and forwards the content of the first response **250** as the second response **255** to the mobile device **205** over the port assigned to the mobile device **205**.

[0044] FIG. **2**A is a block diagram **201** illustrating an example request and response flow through the example system of FIG. **1**. The block diagram **201** includes the proxy **165**, the Internet content provider(s) **170**, the mobile device **205**, the carrier network **230**, and the Internet **240**. The block diagram **201** additionally includes the first request **235**, the second request **245**, the first response **250**, and the second response **255**. Further, the requests and responses of the illustrated example are represented by HTTP request and response headers. The first request **235** is represented by the first HTTP request header **236** and the second request **245** is represented by the second HTTP request header **246**. The first response **250** is represented by the first HTTP response header **251** and the second response **255** is represented by the second HTTP response header **256**.

[0045] The first HTTP request header **236** is the header of a GET request generated by the mobile device **205**. In the illustrated example, the Internet content provider **170** is identified by the absolute Universal Resource Locator (URL) identified in the first line of the first HTTP request header **236** and the address of the proxy **165** and uniquely assigned port are identified by the "Host" line of the first HTTP request header **236**. The host identified in the illustrated example is proxy.MonitoringEntity.com, and the port that the request was made on is 50,000. However, any other address identifying the proxy **165**, and any other port may alternatively be used. For example, the address identifying the proxy **165** may be the Internet Protocol (IP) address of the proxy **165**. In the illustrated example, the absolute URL of the Internet resource is "http://www.weather.com/home.html". However, any other URL may additionally or alternatively be used.

[0046] The proxy **165** receives the first content request **235** and generates the second content request **245**. The second content request **245** is represented by the second HTTP request header **246**. In the illustrated example, the second HTTP request header **246** is a GET request directed to "http://

www.weather.com", and is transmitted over port **80** as no port other than port **80** is identified. The content being requested from "http://www.weather.com" in the illustrated example is "/home.html". The proxy generates the contents of the second request by inspecting the first request **235**. For example, the proxy **165** identifies the requested content of the first request **235** as "http://www.weather.com/home.html", determines that the port to be translated to is port **80** (identified by http://), determines that the Internet content provider **170** identified is "www.weather.com", and determines that the requested webpage from the Internet content provider is "/home.html". The second content request **245** is transmitted over port **80** because the proxy **165** determines that the requested content is HTTP content, and no alternative port number is specified. Alternatively, the content identified by the first content request **235** may be content that is provided on a port other than port **80**. In that example, the absolute URL of the first HTTP request header **236** would identify the requested content as "http://www.weather.com:1234/home.html", to convey that the content identified by the request is provided on port **1234**. Further, the proxy **165** would generate the second HTTP request header **246** and include port **1234** in the identified host (e.g., www.weather.com:1234).

[0047] The Internet content providers **170** receive the second content request **245**, and respond to the request via the first response **250**. The first response **250** is transmitted to the proxy **165**. In the illustrated example, the first response is transmitted over port **80**, as it is a response to a content request made on port **80**. However, any other port may be used to transmit the first response to the proxy **165**. The proxy **165** receives the first response **250**, and determines the correct port that the second response **255** should be transmitted over. In the illustrated example, the proxy **165** determines the port that the second response should be transmitted over by associating the first response **250** with the first request **235** via the second request **245**. In such an example, the proxy **165** can identify that the first request **235** originated on port **50,000**, and thus, the second response should be transmitted on port **50,000**. However, any other method of determining the port to transmit the second response over may additionally or alternatively be used. Further, the response may be transmitted over a port other than the port assigned to the mobile device **205**.

[0048] FIG. **3** is a block diagram of the example proxy **165** of FIG. **1**. The example proxy **165** includes request and response ports **305**, a request servicer **310**, an Internet content processor **315**, a content gatherer **320**, and an Internet port **325**. The request and response ports **305** receive requests and transmit responses to and/or from the client devices **110**, **130**. The requests received by the ports **305** are passed to the request servicer **310**. The content gatherer **320** transmits requests and receives responses from the Internet content providers **170** via the Internet port **325**. The Internet content processor **315** stores the requests (or portions thereof) and/or the retrieved content (or portions thereof or identifiers associated therewith) in the storage database **160**.

[0049] The request and response ports **305** of the illustrated example are Transmission Control Protocol (TCP) ports and/or User Datagram Protocol (UDP) ports. However, any other port-based system may additionally or alternatively be used. The request and response ports of the illustrated example are Dynamic and/or Private Ports as defined by IANA. As such, the ports **305** range from port **49152** to port **65535**, inclusive. However, the ports may use only some of this range (and the used portions may or may not be contiguous) and/or the ports may include ports in any other range such as, for example, Well Defined Ports (ranging from port **0** to port **1023**) and/or Registered Ports (ranging from port **1024** to port **49151**).

[0050] The request servicer **310** of the illustrated example receives the requests from the request and response ports **305** and performs a port translation. A port translation may not be necessary in the event that the proxy is hosted via the same port that the requested content is hosted on. For example, if the proxy is hosted on port **80** and the content request is for content provided on port **80** (e.g., HTTP content), no port translation would occur. First, the request is inspected to determine the destination port that is intended for communication with the Internet content provider **170**. For example, in many situations, the request will be for HTTP content and the destination port will be identified as port **80**. However, any other destination port may be employed. For example, FTP traffic may be translated to port **21**. The content gatherer **320** is responsible for gathering the content identified in the request (e.g., by sending translated requests to the corresponding content provider). Once the content is gathered, the request servicer **310** performs another port translation on the received content response to generate a translated response and to send the translated response to the client device over the port assigned to the client device that made the request.

[0051] The Internet content processor **315** of the illustrated example determines the port (e.g., port **50,000**) that the request was received on, and stores the request in the storage database **160** in association with the port to uniquely identify the client device. Additionally or alternatively, the Internet content processor **315** may use the port number to determine and store the panelist ID and/or the client device ID that was generated by the registrar **155** upon registration. In the illustrated example, the Internet content processor **315** stores the request for content. However, the Internet content processor **315** may store less than the entire request, a symbol for the request, etc., as shown in the tables of FIG. **3**. Additionally or alternatively, the Internet content processor **315** may store the content provided in the response and/or segments and/or portions of the content provided in the response in the storage database **160**. For example, the Internet content processor **315** may store advertisements transmitted to the client device in the storage database **160**.

[0052] The content gatherer **320** of the illustrated example requests the content identified by the request for Internet content. In particular, the content gatherer **320** utilizes the Internet address of the content requested in the request via one of the ports **305** to generate a second request to gather the requested Internet content. The content gatherer **320** transmits the second request via the Internet port **325**. The Internet port **325** of the illustrated example is a Transmission Control Protocol (TCP) port and/or a User Datagram Protocol (UDP) port. However, any other port-based system may additionally or alternatively be used. The Internet port of the illustrated example is for HTTP traffic (e.g., port **80**). However, any other port may be used. For example, port **21** could be used for File Transfer Protocol (FTP) traffic.

[0053] While an example manner of implementing the proxy **165** of FIG. **1** has been illustrated in FIGS. **1** and **3**, one or more of the elements, processes, and/or devices illustrated in FIG. **3** may be combined, divided, re-arranged, omitted, eliminated, and/or implemented in any other way. Further, the request and response ports **305**, the request servicer **310**, the Internet content processor **315**, the content gatherer **320**, the

Internet port **325** and/or, more generally, the example proxy **165** of FIG. **3** and/or the example registrar **155** of FIG. **1** may be implemented by hardware, software, firmware, and/or any combination of hardware, software, and/or firmware. Thus, for example, any of the example request and response ports **305**, the example request servicer **310**, the example Internet content processor **315**, the example content gatherer **320**, the example Internet port **325** and/or, more generally, the example proxy **165** could be implemented by one or more circuit(s), programmable processor(s), application specific integrated circuit(s) (ASIC(s)), programmable logic device (s) (PLD(s)) and/or field programmable logic device(s) (FPLD(s)), etc. When any of the appended apparatus claims are read to cover a purely software and/or firmware implementation, at least one of the example request and response ports **305**, the example request servicer **310**, the example Internet content processor **315**, the example content gatherer **320**, the example Internet port **325**, the example proxy **165**, the example registrar **155**, and/or the storage database **160** are hereby expressly defined to include hardware and/or a computer readable medium such as a memory, DVD, CD, etc. storing the software and/or firmware. Further still, the example proxy **165** of FIGS. **1** and **3** may include one or more elements, processes, and/or devices in addition to, or instead of, those illustrated in FIG. **3**, and/or may include more than one of any or all of the illustrated elements, processes, and devices.

[0054] A flowchart representative of example machine-readable instructions for implementing the proxy **165** of FIGS. **1** and/or **3** is shown in FIG. **4**. Further, a flowchart representative of example machine-readable instructions for implementing the registrar **155** of FIG. **1** is shown in FIG. **5**. In these examples, the machine-readable instructions comprise program(s) for execution by a processor such as the processor **712** shown in the example computer **700** discussed below in connection with FIG. **7**. The program may be embodied in software stored on a computer readable medium such as a CD-ROM, a floppy disk, a hard drive, a digital versatile disk (DVD), or a memory associated with the processor **712**, but the entire program(s) and/or parts thereof could alternatively be executed by a device other than the processor **712** and/or embodied in firmware or dedicated hardware. Further, although the example program(s) are described with reference to the flowcharts illustrated in FIGS. **4** and **5**, many other methods of implementing the example proxy **165** and/or the example registrar **155** may alternatively be used. For example, the order of execution of the blocks may be changed, and/or some of the blocks described may be changed, eliminated, or combined.

[0055] As mentioned above, the example processes of FIGS. **4** and **5** may be implemented using coded instructions (e.g., computer-readable instructions) stored on a tangible computer readable medium such as a hard disk drive, a flash memory, a read-only memory (ROM), a compact disk (CD), a digital versatile disk (DVD), a cache, a random-access memory (RAM) and/or any other storage media in which information is stored for any duration (e.g., for extended time periods, permanently, brief instances, for temporarily buffering, and/or for caching of the information). As used herein, the term tangible computer-readable medium is expressly defined to include any type of computer readable storage and to exclude propagating signals. Additionally or alternatively, the example processes of FIGS. **4** and **5** may be implemented using coded instructions (e.g., computer-readable instructions) stored on a non-transitory computer-readable medium such as a hard disk drive, a flash memory, a read-only memory, a compact disk, a digital versatile disk, a cache, a random-access memory and/or any other storage media in which information is stored for any duration (e.g., for extended time periods, permanently, brief instances, for temporarily buffering, and/or for caching of the information). As used herein, the term non-transitory computer-readable medium is expressly defined to include any type of computer-readable medium and to exclude propagating signals.

[0056] FIG. **4** is a flowchart representative of example machine-readable instructions **400** that may be executed to implement the example proxy of FIGS. **1**, **2**, and **3**. The program of FIG. **4** begins at block **405**, where the example machine-readable instructions **400** begin execution. First, the request servicer **310** of the proxy **165** waits for content requests (block **405**). In the illustrated example, the request servicer **310** waits for content requests only on ports assigned to a client. However, the request servicer **310** may wait for content requests on any or all ports. Additionally, the request servicer **310** may inspect the Internet Protocol (IP) address against known range(s) of IP addresses to determine if the request should be serviced. For example, the known range of IP address may include ranges of IP addresses which are assigned to a particular Internet service provider and/or carrier. This may, for example, restrict use of the proxy **165** to mobile devices. If the request servicer **310** determines that the request did not originate from an IP address within the particular Internet service provider, the request servicer **310** may ignore the request.

[0057] Next, the request servicer **310** receives a content request on a port. Because multiple requests for content may be received at substantially the same time, the proxy **165** may receive a first content request on a first port (block **410**) and a second content request on a second port (block **430**). In the illustrated example, the content requests are processed in parallel to decrease the amount of time taken to respond to requests. However, the content requests may be processed in any other manner. For example, the content requests may be processed serially. The parallel processing of any number of requests is represented in FIG. **4** by these dots "●●●".

[0058] Next, the content gatherer **320** generates second request(s) based on corresponding ones of the request received at blocks **410** and **430**, to retrieve the Internet content identified in the corresponding content requests (blocks **415** and **435**). The content gatherer **320** gathers the requested Internet content by sending the second requests via the Internet port **325**. In the illustrated example, port **80** is used for sending requests. However, any other port may additionally or alternatively be used.

[0059] The Internet content processor **315** also associates the content requests with the corresponding requesting device and stores the association in the storage database (blocks **420** and **440**). In the illustrated example, the Internet content processor **315** associates the first content request with the corresponding client device using the port number that the request was received upon. Since each port is used only by a single client device, each client device can be uniquely identified based on the port number of the port on which a request is received. Further, when storing the association in the storage database **160**, the Internet content processor **315** may store one or more identifier(s) of the port, the client device, the panelist, etc. Additionally, the Internet content processor

315 may store the returned content or a portion of the returned content in the storage database **160** (block **420**, **440**).

[0060] The Internet content processor **315** may filter what is stored in the storage database. For example, the Internet content processor **315** may only store content requests that request HTTP content, as requests for non-HTTP content may not be parsed properly when analyzing the information. As another example, the Internet content processor **315** may omit style content (e.g., cascading style sheet (CSS) documents) from being stored in the storage database **160**, as style content may be of limited use when analyzing the information.

[0061] The request servicer **310** finishes servicing the request from the client device by transmitting the requested Internet content to the client device via the port on which the content request was received (blocks **425** and **445**). Control returns to the block **405**, where the request servicer **310** waits for more content requests (block **405**).

[0062] FIG. **5** is a flowchart representative of example machine-readable instructions **500** that may be executed to implement the example registrar **155** of FIG. **1**. The example machine-readable instructions **500** of FIG. **5** begin execution at block **503**, where the panelist **115**, **135** submits registration data to the registrar **155** (block **503**). In the illustrated example, the registration data is received by the registrar **155** (block **505**) via an electronic interface (e.g., a website). However, the registrar may receive the registration data in any other way. For example, the registrar may receive the registration data via a telephone interface, direct mailings, predefined lists, etc.

[0063] Next, the registrar **155** assigns the panelist a unique port (block **510**). In the illustrated example, the unique port is within the Dynamic and/or Private Port range as defined by IANA (e.g., port **49152** through **65535**). However, any other port number in any other range may alternatively be used. In the illustrated example, because ports are assigned on a one panelist to one port basis, the port number functions as a unique identifier for the client device and/or the panelist.

[0064] The registrar **155** generates a configuration file (block **515**). The configuration file includes the unique port assigned to the client device of the panelist, and an Internet proxy address. The Internet proxy address is the address of the proxy **165**. The port number is a port of the proxy **165** and is uniquely associated with the panelist. In the illustrated example, the configuration document is an Extensible Markup Language (XML) file implementing a property list (plist) file comprising configuration data including the port number and the Internet proxy address. However, any other type of document may be generated such as, for example, a comma separated (CSV) document, a portable document format (PDF) document, a Microsoft® Word® document, etc. In the illustrated example, the configuration document is signed using a public/private key infrastructure. However, the configuration may alternatively not be signed. If the configuration document is not signed, it may appear as an invalid configuration file to the panelist, which may cause the panelist to abandon participation in the panel.

[0065] Next, the registrar **155** transmits the configuration file to the client device (block **520**). In the illustrated example, the configuration file is transmitted via an electronic mail (email) message. The email message includes a hyperlink that may be selected to download the configuration file. However, any other methods of transmitting the configuration file may additionally or alternatively be used. For example, the configuration file may be transmitted as an attachment to the email message, the registrar **155** may transmit a short message service (SMS) message comprising an Internet address where the client device may download the configuration file, a direct mailing may be sent to the panelist comprising the instruction document and/or additionally comprising an electronic medium containing the configuration file, a telephone call may be placed to orally instruct the panelist on how to configure the client device, etc. The panelist and/or client device then receives the configuration file (block **523**).

[0066] The client device **110**, **130** is then configured via the configuration file (block **525**). Since the configuration file is an electronic document that may be interpreted by the client device **110**, **130**, the client device receives the transmitted configuration file and automatically applies the settings contained in the document such that further Internet requests originating with the client are addressed to the corresponding port of the proxy **165**. However, the configuration file may additionally or alternatively include an instruction document that may guide the panelist on how to configure the client device. The instruction document may thereby instruct the panelist on how to apply the configuration file or may instruct the panelist on how to manually apply the data in the configuration file.

[0067] Upon application of the data contained in the configuration file, subsequent requests for Internet content made by the client device **110**, **130** are routed according to the configuration file. In particular, since the configuration file includes the Internet proxy address and the unique port number assigned to the client device, requests are proxied through the Internet proxy address via the unique port number.

[0068] FIG. **6** illustrates an example configuration file **600** that may be generated by the example registrar **155** of FIG. **1**. The example configuration file **600** includes configuration data **605**. The configuration data **605** include an Internet proxy address **610** and a unique port assignment **615**.

[0069] The configuration file **600** is an Extensible Markup Language (XML) file implementing a property list (plist) file including configuration data such as the port number and the Internet proxy address of the proxy **165**. However, any other type of document may be generated such as, for example, a comma separated (CSV) document, a portable document format (PDF) document, a Microsoft® Word® document, etc. The configuration file is implemented as a plist file in the illustrated example to facilitate support for an Apple® iPhone® as the mobile device. However, any other mobile device may additionally or alternatively be used, and the mobile device may implement any other operating system (e.g., Google® Android, Windows® Mobile®, etc.). For example, the configuration file may be formatted differently or may be in a different format to support interpretation by client devices implementing an operating system other than the operating system implemented by the Apple® iPhone®.

[0070] FIG. **7** is a block diagram of an example computer **700** capable of executing the instructions of FIGS. **4** and **5** to implement the monitoring system of FIG. **1**. The computer **700** can be, for example, a server, a personal computer, or any other type of computing device.

[0071] The system **700** of the instant example includes a processor **712**. For example, the processor **712** can be implemented by one or more Intel® microprocessors from the Pentium® family, the Itanium® family or the XScale® family. Of course, other processors from other families are also appropriate.

[0072] The processor **712** is in communication with a main memory including a volatile memory **718** and a non-volatile memory **720** via a bus **722**. The volatile memory **718** may be implemented by Synchronous Dynamic Random Access Memory (SDRAM), Dynamic Random Access Memory (DRAM), RAMBUS Dynamic Random Access Memory (RDRAM) and/or any other type of random access memory device. The non-volatile memory **720** may be implemented by flash memory and/or any other desired type of memory device. Access to the main memory **714** is typically controlled by a memory controller (not shown).

[0073] The computer **700** also includes an interface circuit **724**. The interface circuit **724** may be implemented by any type of interface standard, such as an Ethernet interface, a universal serial bus (USB), and/or a PCI express interface.

[0074] One or more input devices **726** are connected to the interface circuit **724**. The input device(s) **726** permit a user to enter data and commands into the processor **712**. The input device(s) can be implemented by, for example, a keyboard, a mouse, a touchscreen, a track-pad, a trackball, isopoint and/or a voice recognition system.

[0075] One or more output devices **728** are also connected to the interface circuit **724**. The output devices **728** can be implemented, for example, by display devices (e.g., a liquid crystal display, a cathode ray tube display (CRT), a printer and/or speakers). The interface circuit **724**, thus, typically includes a graphics driver card.

[0076] The interface circuit **724** also includes a communication device (e.g., the request servicer **310**) such as a modem or network interface card to facilitate exchange of data with external computers via a network (e.g., an Ethernet connection, a digital subscriber line (DSL), a telephone line, coaxial cable, a cellular telephone system, etc.).

[0077] The computer **700** also includes one or more mass storage devices **730** for storing software and data. Examples of such mass storage devices **730** include floppy disk drives, hard drive disks, compact disk drives, and digital versatile disk (DVD) drives. The mass storage device **730** may implement the storage database **160**.

[0078] The coded instructions **732** of FIGS. **4** and **5** may be stored in the mass storage device **730**, in the volatile memory **718**, in the non-volatile memory **720**, in the local memory **714**, and/or on a removable storage medium such as a CD or DVD.

[0079] From the foregoing, it will be appreciated that example methods, apparatus and articles of manufacture have been disclosed which allow Internet content requests made from mobile devices without requiring authorization credentials while still uniquely identifying the requesting device and/or panelist irrespective of whether the request originated with a browser or an application accessing Internet content.

[0080] Although certain example methods, apparatus, and articles of manufacture have been described herein, the scope of coverage of this patent is not limited thereto. On the contrary, this patent covers all methods, apparatus, and articles of manufacture fairly falling within the scope of the claims of this patent.

1. A method to monitor Internet activity comprising:

receiving a request for Internet content on a port of a proxy, the request originating from a mobile device transmitting requests via a cellular wireless access point;

associating the request for Internet content with a mobile device based on an identifier of the first port;

requesting content from an Internet content provider identified in the request for Internet content, the Internet content provider being different than the proxy; and

transmitting the content.

2. The method as defined in claim **1**, wherein transmitting the content comprises transmitting the content via the first port.

3. The method as defined in claim **1**, further comprising storing the request for Internet content in a database.

4. The method as defined in claim **1**, further comprising storing the requested Internet content in a database.

5. The method as defined in claim **1**, further comprising not servicing the request for Internet content if the request originated from an Internet Protocol address outside of an IP address range.

6. The method as described in claim **5**, wherein the IP range is a range of IP addresses representing devices on a cellular network.

7. The method as described in claim **1**, wherein the port is within a range of at least one of dynamic and private ports.

8. The method as described in claim **1**, wherein requests for Internet content are received on a number of ports of the proxy corresponding to a number of panelists in a panel.

9. The method as described in claim **8**, wherein the panel comprises sixty panelists.

10. The method as described in claim **8**, wherein the panel comprises fifteen hundred panelists.

11. The method as described in claim **1**, wherein the request for Internet content is un-authenticated.

12. A method to monitor Internet activity, the method comprising:

designating a first client device to transmit content requests via a first port of a proxy;

designating a second client device to transmit content requests via a second port of the proxy, the second port being different from the first port;

receiving a first content request on the first port from the first client device;

receiving a second content request on the second port from the second client;

transmitting first content identified by the first content request to the first client device;

transmitting second content identified by the second content request to the second client device; and

storing an identifier of the first content requested by the first content request in association with the first client devices based on an identity of the first port.

13. The method as described in claim **12**, further comprising storing a portion of the first content in association with the first client device.

14. The method as described in claim **12**, wherein storing the identifier of the first content requested by the first content request further comprises associating a first panelist identifier associated with the first client device with the identifier of the first content.

15. The method as described in claim **14**, wherein the first panelist identifier is an identifier of the first port.

16. The method as described in claim **12**, wherein designating the first client device to transmit content requests via the first port further comprises transmitting an identifier of the first port and an Internet address of the proxy to the first client device to cause the first client device to transmit subsequent requests for content to the first port of the proxy.

17. The method as described in claim **16**, wherein transmitting the first port identifier and the Internet address of the proxy further comprises generating a configuration file containing the first port identifier and the Internet address of the proxy.

18-26. (canceled)

27. A method to monitor Internet activity, the method comprising:

assigning a number of different mobile devices to communicate with respective ones of a number of different ports of a proxy server, the number of mobile devices and number of ports corresponding to a number of panelists in a panel;

receiving an un-authenticated request for Internet content via one of the number of mobile devices based on the number of ports; and

using the one of the number of ports to identify the mobile device associated with the request.

28. The method as described in claim **27**, wherein the panel comprises at least sixty panelists.

29. The method as described in claim **27**, wherein the panel comprises at least fifteen hundred panelists.

30. The method as described in claim **27**, wherein the number of ports are within a range from port **49152** to port **65535**.

31. The method as described in claim **27**, further comprising storing an identification of the content requested by the request in association with the identified client device.

32-43. (canceled)

* * * * *