SESSION CONTINUITY FOR PROVIDING CONTENT TO A REMOTE DEVICE

Inventors: Yingqing L. Cui, San Jose, CA (US); Min Zhou, Palo Alto, CA (US); Zhaowei C. Jiang, San Jose, CA (US)

Correspondence Address:
DARBY & DARBY P.C.
P.O. BOX 5257
NEW YORK, NY 10150-6257 (US)

Assignee: Yahoo! Inc., Sunnyvale, CA (US)

Appl. No.: 11/027,747

Filed: Dec. 30, 2004

Related U.S. Application Data

Continuation-in-part of application No. 10/951,982, filed on Sep. 28, 2004.

Publication Classification

Int. Cl. G06F 17/30 (2006.01)

U.S. Cl. .................................................................................. 707/10

ABSTRACT

A method and apparatus is directed to provide a clip of content to a remote device, such as a mobile device. The invention enables an end-user to select content from a networked device, such as a personal computer. The selected content may include content from a webpage, graphic images, audio files, and the like. Selecting the content includes entry of an identifier such as a Mobile Identification Number (MIN), and a Mobile Station International ISDN Number (MSISDN). When the end-user employs the remote device to access the content, a server employs the identifier to determine if the remote device is authenticated and authorized to access the content. If it is, then the server provides the content to establish session continuity with the remote device. The content may then be transmitted to the remote device using any of a variety of messaging protocols.

```
START

Determine Desired Content

Select Clip of Content

Provide Identifier for Remote Session

Request Clipped Content be sent towards Remote Device

Clip More Content?

YES

NO

RETURN
```
FIG. 1

Wireless Network

Client Device

Remote Device

Wide Area Network/Local Area Network

Content Server
START

Determine Desired Content

Select Clip of Content

Provide Identifier for Remote Session

Request Clipped Content be sent towards Remote Device

Clip More Content?

YES

NO

RETURN

FIG. 3
START

Receive Content

Receive Identifier for Remote Device

Associate Content With Identifier of Remote Device

Send Message to Remote Device Regarding Content

Request From Remote Device?

YES

Receive Identifier from Remote Device

Valid Authentication? (Fig. 5)

YES

Retrieve Content Using Identifier

Provide Content To Remote Device

RETURN

NO

FIG. 4
START

Highly Sensitive Content? - YES → Identifier Matches Pre-Registered Remote Device - NO

NO

Sensitive Content? - YES → Log-in Matches Remote Log-in - NO

NO

Content Includes DRMs? - YES → Remote Device 1st Claimed Content? - NO

NO

Time Period Expired? - YES → Request is Unauthorized

NO

Request is Authorized

RETURN

FIG. 5
FIG. 6

START

Perform Action on Received Content 602

Send Action and/or Content Status to Server 604

Update Session Data Using Received Action and/or Content Status 606

Provide Updated Session Data to Client Device 608

RETURN
SESSION CONTINUITY FOR PROVIDING CONTENT TO A REMOTE DEVICE

RELATED APPLICATIONS


FIELD OF THE INVENTION

[0002] The invention relates generally to managing content over a network, and more particularly but not exclusively to an apparatus and method for providing content clipped from a networked source to a mobile device, using message session continuity.

BACKGROUND OF THE INVENTION

[0003] In today’s computing environment, a user may employ a variety of computing devices. For example, a user may use a desktop personal computer (PC) at a fixed workplace, at home, or the like. However, the same user may use a mobile computing device, such as a cellular telephone, a palm-size PC, and perhaps even a personal data assistant (PDA) during travel.

[0004] With such a variety of computing devices, there is a desire to be able to share information across the computing devices. Today, there is some limited capability to share data though a mechanism known as data synchronization. However, this mechanism often requires the two devices to be physically collated, and often networked, for the data to be transferred.

[0005] Moreover, as the users transitions between various computing devices, such as their PC and their mobile computing devices, information associated with their PC session may not be available during their mobile session. Thus session continuity between the computing devices may be lost. It is, thus, with respect to these considerations and others that the present invention has been made.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Non-limiting and non-exhaustive embodiments of the invention are described with reference to the following drawings. In the drawings, like reference numerals refer to like parts throughout the various figures unless otherwise specified.

[0007] For a better understanding of the invention, reference will be made to the following Detailed Description of the Invention, which is to be read in association with the accompanying drawings, wherein:

[0008] FIG. 1 shows a functional block diagram illustrating one embodiment of an environment for practicing the invention;

[0009] FIG. 2 shows one embodiment of a client device that may be employed in a system implementing the invention;

[0010] FIG. 3 illustrates a logical flow diagram generally showing one embodiment of a process for selecting content for delivery to a remote device using session continuity;

[0011] FIG. 4 illustrates a logical flow diagram generally showing one embodiment of a process for managing delivery of content to the remote device with session continuity;

[0012] FIG. 5 illustrates a logical flow diagram generally showing one embodiment of a process for authenticating a remote device for access to the content; and

[0013] FIG. 6 illustrates a logical flow diagram generally showing one embodiment of a process for providing action and/or content status to a client device using session continuity, in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0014] The present invention now will be described more fully hereinafter with reference to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific exemplary embodiments by which the invention may be practiced. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Among other things, the present invention may be embodied as methods or devices. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

[0015] Briefly stated, the present invention is directed towards a method and apparatus for providing session continuity with a remote device, such as a mobile device. The invention enables an end-user to determine content from a networked device, such as a personal computer. The determined content may have associated with it pre-determined digital access and/or usage rights. Selecting the content for deliver to the remote device may result in a pop-up window, field entry, or the like, that enables entry of an identifier associated with the remote device. This identifier may include a Mobile Identification Number (MIN), a Mobile Station International ISDN Number (MSISDN), Media Access Control (MAC) address, Internet Protocol (IP) address, email address, phone number, and the like. The content is stored on a server and may be linked back to the identifier. Additional session data may also be stored on the server, including, a user identifier, login status, a time stamp, digital rights information, an action, a Uniform Resource Locator (URL), and similar information. In one embodiment, the session data may include multiple time stamps, including an access time, a sign-in time, a content subscription time, and the like. In another embodiment, the session data may include multiple actions, multiple URLs, and so forth, storable within a session record. When the end-user employs the remote device to access the content, the remote device provides an identifier. The server employs the provided identifier from the remote device, and the additional session data to authenticate the remote device and to determine if it is authorized to access the content. If the remote device is authenticated and authorized to access the content, the server provides the stored content to the remote device to establish session continuity between the remote device and the networked device. The content may be transmitted
to the remote device using any of a variety of messaging protocols, including an asynchronous messaging protocol. For example, in one embodiment, the content is transmitted using a Short Message Service (SMS) message. In another embodiment, an SMS message is employed that includes a message hook, including a Universal Resource Locator (URL), to the content.

Illustrative Operating Environment

**FIG. 1** shows components of an exemplary environment in which the invention may be practiced. Not all the components may be required to practice the invention, and variations in the arrangement and type of the components may be made without departing from the spirit or scope of the invention. As shown, system **100** of **FIG. 1** includes client computer **104**, local area networks (“LANs”)/wide area networks (“WANs”) **105**, wireless network **110**, content server **108**, and remote devices **106-107**.

Generally, remote devices **106-107** may include virtually any computing device capable of connecting to another computing device and receiving information. Such devices include portable devices such as, cellular telephones, smart phones, display pagers, radio frequency (RF) devices, infrared (IR) devices, Personal Digital Assistants (PDAs), handheld computers, wearable computers, tablet computers, integrated devices combining one or more of the preceding devices, and the like. Remote device **106-106** may also include other computing devices, such as personal computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, and the like. As such, remote devices **106-107** typically range widely in terms of capabilities and features. For example, a cell phone may have a numeric keypad and a few lines of monochrome LCD display on which only text may be displayed. In another example, a web-enabled remote device may have a touch sensitive screen, a stylus, and several lines of color LCD display in which both text and graphics may be displayed. Moreover, the web-enabled remote device may include a browser application enabled to receive and to send wireless application protocol messages (WAP), and the like. In one embodiment, the browser application is enabled to employ Handheld Device Markup Language (HDML), Wireless Markup Language (WML), WMLScript, JavaScript, EXTensible HTML (xHTML), Compact HTML (CHTML), and the like, to display and send a message.

Remote devices **106-107** also may include at least one client application that is configured to receive content from another computing device. The client application may include a capability to provide and receive textual content, graphical content, audio content, alerts, messages, and the like.

Remote devices **106-107** may further provide information that identifies itself, including a type, capability, name, identifier, and the like. For example, remote devices **106-107** may provide a message, network packet, and the like, that includes a Mobile Identification Number (MIN), a Mobile Station, International ISDN Number (MSISDN), and the like. A MIN may include a North American Numbering Plan (NANP) number that is configured to serve as a mobile telephone number for remote devices **106-107**. MINS may be programmed into remote devices **106-107**, at time of manufacture, purchase, and the like. In one embodiment, remote devices **106-107** may employ a different identifier based on a type of message communication employed. For example, remote devices **106-107** may employ a MIN identifier for a WAP request, and a MSISDN for an SMS message. Remote devices **106-107** are not limited to MINS, and MSISDNs, however, and virtually any other identifier may be provided, such as an electronic serial number (ESN), application serial number, a MAC address, IP address, an email address, message address, and the like, without departing from the scope of the invention. Remote devices **106-107** may also provide information that indicates a content format that the remote device **106-107** is enabled to employ. Such information may be provided in a message, or the like, sent to content server **108**, and the like.

Remote devices **106-107** may be configured to communicate a message, such as through a Short Message Service (SMS), Multimedia Message Service (MMS), instant messaging (IM), internet relay chat (IRC), mIRC, Jabber, and the like, between another computing device, such as content server **108**, and the like. In one embodiment, the message includes a message hook, such as a URL, script, program, and the like. Remote devices **106-107** may be further configured to employ the message hook to request access to another message, such as from content server **108**, and the like. In one embodiment, the other message is an email message. In another embodiment, the other message is an email message that is formatted in a Wireless Application Protocol (WAP) format, and the like. However, the present invention is not limited to email messages, and virtually any other message type, and the like, may be accessible through the included message hook. For example, the message may include, but not be limited to, a document, an audio file, a graphics file including a bitmap file, a jpeg file, a binary file, a video file, a File Transfer Protocol command, a compressed file, a document, a script, an application, an alert, and the like.

Remote devices **104** may include virtually any computing device capable of receiving and sending a message over a network, such as network **105**, wireless network **110**, and the like, to and from another computing device, such as content server **108**, remote devices **106-107**, and the like. The set of such devices may include devices that typically connect using a wired communications medium such as personal computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, and the like. The set of such devices may also include devices that typically connect using a wireless communications medium such as cell phones, smart phones, pagers, walkie talkies, radio frequency (RF) devices, infrared (IR) devices, CIs, integrated devices combining one or more of the preceding devices, or virtually any mobile device, and the like. Similarly, client device **104** may be any device that is capable of connecting using a wired or wireless communications medium such as a PDA, POCKET PC, wearable computer, and any other device that is equipped to communicate over a wired and/or wireless communications medium.

Client device **104** may include a browser application that is configured to receive and to send web pages, web-based messages, and the like. The browser application may be configured to receive and display graphics, text, multimedia, and the like, employing virtually any web based language, including Standard Generalized Markup Language (SMGL), such as HyperText Markup Language (HTML), and so forth.
Client device 104 may further include a client application that enables it to perform a variety of other actions, including communicating a message, such as through a Short Message Service (SMS), Multimedia Messaging Service (MMS), Instant Messaging (IM), Internet Relay Chat (IRC), mIRC, Jabber, and the like, between itself and another computing device. The browser application, and/or another application, such as the client application, a plug-in application, and the like, may enable client device 104 to select content to be clipped, reformatted, and delivered to a remote device, such as remote devices 106-107. Moreover, the client application, plug-in, browser page, and the like, may enable client device 104 to provide an identifier associated with the remote device, so that a session may be maintained between client device 104 and the remote device. The provided identifier may include virtually any identifier associated with the destination remote device, including a MIN, MSISDN, ESN, MAC address, IP address, email address, message address, and the like. Moreover, client device 104 may enable additional information to be provided about the session, including a user identifier, a login status, and so forth. In one embodiment, client device 104 may be configured to perform actions such as described below in conjunction with FIG. 3 to select, and provide the content for delivery to the remote device.

Wireless network 110 is configured to couple remote device 106 and its components with WAN/LAN 102. Wireless network 110 may include any of a variety of wireless sub-networks that may further overlay stand-alone ad-hoc networks, and the like, to provide an infrastructure-oriented connection for remote device 106. Such sub-networks may include mesh networks, Wireless LAN (WLAN) networks, cellular networks, and the like.

Wireless network 110 may further include an autonomous system of terminals, gateways, routers, and the like connected by wireless radio links, and the like. These connectors may be configured to move freely and randomly and organize themselves arbitrarily, such that the topology of wireless network 110 may change rapidly.

Wireless network 110 may further employ a plurality of access technologies including 2nd (2G), 2.5, 3rd (3G), 4th (4G) generation radio access for cellular systems, WLAN, Wireless Router (WR) mesh, and the like. Access technologies such as 2G, 3G, and future access networks may enable wide area coverage for mobile devices, such as remote device 106 with various degrees of mobility. For example, wireless network 110 may enable a radio connection through a radio network access such as Global System for Mobil communication (GSM), General Packet Radio Services (GPRS), Enhanced Data GSM Environment (EDGE), Wideband Code Division Multiple Access (WCDMA), CDMA2000, and the like. In essence, wireless network 110 may include virtually any wireless communication mechanism by which information may travel between remote device 106 and another computing device, network, and the like.

Network 105 is configured to couple content server 108 and its components with other computing devices, including remote device 107, client computer 104, content server 108, and through wireless network 110 to remote device 106. Network 105 is enabled to employ any form of computer readable media for communicating information from one electronic device to another. Also, network 105 can include the Internet in addition to local area networks (LANs), wide area networks (WANs), direct connections, such as through a universal serial bus (USB) port, other forms of computer-readable media, or any combination thereof. On an interconnected set of LANs, including those based-on differing architectures and protocols, a router acts as a link between LANs, enabling messages to be sent from one to another. Also, communication links within LANs typically include twisted wire pair or coaxial cable, while communication links between networks may utilize analog telephone lines, full or fractional dedicated digital lines including T1, T2, T3, and T4, Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs), wireless links including satellite links, or other communications links known to those skilled in the art. Furthermore, remote computers and other related electronic devices could be remotely connected to either LANs or WANs via a modem and temporary telephone link. In essence, network 105 includes any communication method by which information may travel between content server 108 and another computing device.

Additionally, communication media typically embodies computer-readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave, data signal, or other transport mechanism and includes any information delivery media. The terms “modulated data signal,” and “carrier-wave signal” includes a signal that has one or more of its characteristics set or changed in such a manner as to encode information, instructions, data, and the like, in the signal. By way of example, communication media includes wired media such as twisted pair, coaxial cable, fiber optics, wave guides, and other wired media and wireless media such as acoustic, RF, infrared, and other wireless media.

One embodiment of content server 108 is described in more detail below in conjunction with FIG. 2. Briefly, however, content server 108 may include any computing device capable of connecting to network 105 to enable a user of client device 104 to establish session continuity with a remote device to, for example, provide content for delivery to the remote device. The session may be established using an identifier associated with the remote device. Devices that may operate as content server 108 include personal computers desktop computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, servers, and the like. Content server 108 may employ process 400 of FIG. 4 to perform content services between client device 104 and the identified remote device. Illustrative Server Environment

FIG. 2 shows one embodiment of a server device, according to one embodiment of the invention. Server device 200 may include many more components than those shown. The components shown, however, are sufficient to disclose an illustrative embodiment for practicing the invention. Server device 200 may, for example, be employed to operate as content server 108 of FIG. 1.

Server device 200 includes processing unit 212, video display adapter 214, and a mass memory, all in communication with each other via bus 222. The mass memory generally includes RAM 216, ROM 232, and one or more permanent mass storage devices, such as hard disk.
drive 228, tape drive, optical drive, and/or floppy disk drive. The mass memory stores operating system 220 for controlling the operation of server 102. Any general-purpose operating system may be employed. Basic input/output system ("BIOS") 218 is also provided for controlling the low-level operation of server device 200. As illustrated in FIG. 2, server device 200 also can communicate with the Internet, or some other communications network, such as network 105 and wireless network 110 in FIG. 1, via network interface unit 210, which is constructed for use with various communication protocols including TCP/IP protocol, UDP/IP protocol, and the like. Network interface unit 210 is sometimes known as a transceiver, transceiving device, network interface card (NIC), and the like.

[0032] Server device 200 may also include an SMTP handler application for transmitting and receiving email. Server device 200 may also include an HTTP handler application for receiving and handling HTTP requests, and an HTTPS handler application for handling secure connections. The HTTPS handler application may initiate communication with an external application in a secure fashion.

[0033] Server device 200 also includes input/output interface 224 for communicating with external devices, such as a mouse, keyboard, scanner, or other input devices not shown in FIG. 2. Likewise, server device 200 may further include additional mass storage facilities such as CD-ROM/ DVD-ROM drive 226 and hard disk drive 228. Hard disk drive 228 is utilized by server device 200 to store, among other things, application programs, and the like.

[0034] The mass memory as described above illustrates another type of computer-readable media, namely computer storage media. Computer storage media may include volatile, nonvolatile, removable, and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. Examples of computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by a computing device.

[0035] The mass memory also stores program code and data. One or more applications 250 are loaded into mass memory and run on operating system 220. Examples of application programs include email programs, schedulers, calendars, security services, transcoders, database programs, word processing programs, spreadsheet programs, and so forth. Mass storage may further include applications such as web services 252, content manager 254, session data 256, and content store 258. Although not illustrated, a user store may also be included for storing and managing end-user data, including email addresses, message addresses, phone numbers, name, place of residence information, billing information, and the like.

[0036] Web services 252 are configured to manage requests from a client device's browser application and deliver web-based content in response. As such, web services 252 may include such applications as Apache, Internet Information Server (IIS), Netscape, National Center for Supercomputing Applications (NCSA), and the like. In one embodiment, web services 252 communicate with the client's browser application employing HTTP. However, web services may also execute server-side scripts (CGI scripts, JSPs, ASPs, and so forth) that provide functions such as database searching, e-commerce, and the like. In one embodiment, web services 252 interacts with content manager 254 to enable clipping of content provided to the client's browser for delivery to another computing device. In one embodiment, web services 252 may enable a clip icon, drop-down menu, pop-up menu, or similar clip mechanism that allows an end-user to select the content for delivery. Web services 252 may receive the clip mechanism from content manager 254. The clip mechanism may further enable the end-user to provide an identifier that uniquely indicates a remote device to which the clipped content is to be delivered.

[0037] Content manager 254 is configured to receive the content from web services 252, along with the identifier associated with the remote device. Content manager 254 may store the content within content store 258, with a link to the stored content within session data store 256.

[0038] Content manager 254 may further determine a format that is compatible with the identified remote device, and if necessary, content manager 254 may reformat the received content into a compatible format. Content manager 254 may further employ the provided identifier to deliver the reformatted content to the remote device. In one embodiment, content manager 254 may send the reformatted content to the remote device using any of a variety of message protocols, including SMS, SIP, IM, WAP, and the like. In another embodiment, content manager 254 may send a message to the remote device, wherein the message includes a hook, or similar mechanism, that indicates where the clipped content may be obtained. For example, in one embodiment, the hook may include a URL that further includes link to the content on a server. In one embodiment, the link includes the identifier associated with the remote device. When the end user of the remote device receives the message and selects the hook, the content is accessed using the link, and displayed employing the remote device's browser, or other appropriate application. For example, where the content includes text, such as driving instructions, webpage content, and the like, the appropriate application might include the client's browser, word processor, or the like. In any event, content manager 254 may, in one embodiment, employ process 400 of FIG. 4 and interact with process 300 of FIG. 3.

[0039] Session data store 256 may include session records with session data that is associated with a given session. For example, session data may include an identifier, phone number, user identifier, log-in status information, a time stamp, digital rights management information associated with a user and/or content, user identifier associated with the session, a URL, a link to content in content store 258 for the given session, and so forth. In one embodiment, the digital rights management information includes information associated with whether the content is copy-protected, whether the content is to be paid for by an end-user, whether the content has been paid for, and for how many copies, whether the content is highly sensitive, such that only a particular end-user on a particular remote device is authorized to access the content, and so forth. As such, session data store
may be implemented using virtually any storage mechanism, including a file, folder, database, and so forth.

[0040] Content store 258 includes virtually any storage mechanism, including a file, folder, database, and the like, for storing and managing content. In one embodiment, the content is linked back to one or more session records within session data store 256.

[0041] Although illustrated in FIG. 2 as distinct components in server device 200, web services 252, content manager 254, session data store 256 and content store 258 may be arranged, combined, and the like, in any of a variety of ways, without departing from the scope of the present invention. For example, web services 252 and content manager 254 may be arranged as a single component. Moreover, web services 252, content manager 254, session data store 256, and content store 258 may reside in one or more separate computing devices, substantially similar to server device 200. As another example, a distinct data server, similar to server device 200, may be employed, wherein session data store 256 may be managed.

Generalized Operation

[0042] The operation of certain aspects of the present invention will now be described with respect to FIG. 3. FIG. 3 illustrates a logical flow diagram generally showing one embodiment of a process for selecting content for delivery to a remote device using session continuity. Process 300 of FIG. 3 may, for example, represent an interaction between a client device, such as client device 104, and a server device, such as content server 108.

[0043] Process 300 begins, after a start block, at block 302, after an end-user employing a computing device, such as client device 104 of FIG. 1, accesses content over a network. In one embodiment, the content is accessed by the client device using a web browser.

[0044] As an illustrative example, an end-user may wish to provide to a remote device a set of driving directions to a particular point of interest, although the end-user’s client computing device is not currently networked with the remote device. The end-user may employ the client’s web browser to access a website on a server, and request the desired driving directions. Clearly, however, the invention is not limited to displayed content, and other content may be determined, including audio files, movies, graphical files, binary files, and the like.

[0045] Processing then flows to block 304, where the end-user may employ a variety of clip mechanisms to select and clip the desired content. The clip mechanisms employed may include, for example, a button on a toolbar such as a browser toolbar, a link accessible through the browser, a displayed icon, an executable application, script, and the like. In one embodiment, the clip mechanism may reside on a server and be displayed for use through the client’s browser. Thus, in one embodiment, no permanent modifications, or additional permanent applications need reside on the client device. In any event, the end-user might select the clip mechanism, which in turn, captures the determined content. In the present example, the clip mechanism clips the displayed driving instructions.

[0046] Process 300 continues to block 306, where the clip mechanism, or related application, requests the end-user to enter an identifier associated with the remote device. In our example, the end-user may desire to provide the driving instructions to a mobile device, or similar remote device. In this example, the user might include a phone number, MIN, MSISDN, ESN, email address, or similar identifier to uniquely identify the remote device for which delivery of the content is intended. In one embodiment, the identifier is an IP address associated with the remote device.

[0047] Also at block 306, additional session data may be provided to the server for storage. For example, if the content should be treated as highly sensitive information, then such information is also provided to the server for storage. This may arise, for example, where the content was obtained from an end-user’s address book, a financial application, and the like. Similarly, if the content includes digital rights, such digital rights may also be provided. For example, the content may include a graphic that may be downloaded only a limited number of times, within a limited time period, by a particular remote device, and the like. Such digital rights management (DRM) information may therefore also be provided.

[0048] Process 300 flows to block 308, where the end-user then employs the clip mechanism, or a similar mechanism, to request that the clipped content be delivered to the identified remote device. Processing continues next to decision block 310 where a determination is made whether more content is to be clipped for delivery. If no additional content is to be clipped, process 300 returns to a calling process to perform other actions. If additional content is to be clipped, process 300 loops back to block 302 and perform substantially as described above.

[0049] FIG. 4 illustrates a logical flow diagram generally showing one embodiment of a process or managing delivery of content to the remote device with session continuity, in accordance with the present invention. Process 400 of FIG. 4 may, for example, be implemented on a server, such as content server 108 of FIG. 1.

[0050] Process 400 begins, after a start block, at block 402, where content that has been clipped for delivery to another computing device is received. The other computing device may, for example, include remote devices 106-107 of FIG. 1. Moreover, the content may have been clipped using process 300 of FIG. 3 above. Processing then continues to block 404, where an identifier associated with the remote device to receive the content is received. Such identifier enables the remote device to establish a connection with a server, in a manner that establishes session continuity between the clipping computing device (e.g., such as from FIG. 3) and the remote device.

[0051] Processing continues next to block 406, where the received content may be associated with the identifier of the remote device. Moreover, in one embodiment, the identifier may be employed to determine a characteristic of the remote device. In one embodiment, the identifier may be used to search a data base, text, file, and the like, to determine a content format that is compatible with the remote device. In another embodiment, the identifier may be employed to send a query to the remote device to ascertain a compatible format for the content. Upon determination of a compatible format, the content may be formatted using the compatible format. In our present driving instruction example, the content may be formatted into an SMS message. In another embodiment,
the content may be formatted for display in a browser format using HTML, WML, WMLScript, JavaScript, and the like. Similarly, the content may be formatted using a compatible audio format, graphical format, or other format as appropriate for the content type and the remote device.

[0052] In one embodiment, a message hook, such as a URL, script, program, and the like, may be inserted into a messaging mechanism, such as an SMS message, where the message hook may include the identifier associated with the remote device, a link to the content, and the like. When the SMS message is received by the remote device, the message hook may be selected triggering access the content.

[0053] The invention, however, is not constrained to these mechanisms, and virtually any messaging mechanism may be selected to package the formatted content for delivery. For example, the content may be delivered through email, HTTP, IM, MMS, and the like.

[0054] Moreover, additional session data may also be associated with the content at block 406. Such additional session data, including user identifier, log-in status, time stamps, digital rights information, authentication levels, and so forth may be associated with the content. This additional session data may be linked to the content employing any of a variety of mechanisms.

[0055] Process 400 continues next to decision block 408, where a determination is made whether the remote device requests access to the server. In one embodiment, access may be sought when the remote device searches for messages, and the like. In any event, if the remote device does not requesting access, process 400 loops back through decision block 408, until the remote device is requests access. When the remote device does requests access, processing flows to block 412.

[0056] At block 412, the identifier associated with the remote device is received. Again, this identifier may include a MIN, MSISDN, ESN, MAC address, IP address, email address, and the like. Moreover, in one embodiment, additional session information may also be received, including a capability associated with the remote device, log-in status, and so forth.

[0057] Processing flows next to decision block 414, which is described in more detail below in conjunction with FIG. 5. Briefly, however, at decision block 414, a determination is made whether the remote device is sufficiently authenticated and authorized to access the content. If the remote device is unauthorized or does not receive a valid authentication, processing returns to a calling process to perform other actions, such as sending an error message, and the like, to the networked device, and/or the remote device.

[0058] Alternatively, if the remote device is authenticated and is authorized to access the content, processing flows next to block 412, where the received identifier is employed to retrieve the content. Process 400 continues next to block 414, where the content is provided to the remote device, virtually establishing session continuity between the session events on the original computing device and the remote device. Upon delivery of the content, process 400 returns to the calling process to perform other actions.

[0059] FIG. 5 illustrates a logical flow diagram generally showing one embodiment of a process for authenticating a remote device for access to the content. Process 500 of FIG. 5 may be executed from decision block 414 of FIG. 4.

[0060] Process 500 begins, after a start block, at decision block 502, where a determination is made whether the content is pre-determined as highly sensitive. Content may be pre-determined to be highly sensitive employing a variety of mechanisms, such as when the content is clipped, an associated application, and the like, may be determined the content. Similarly, the type of content may have associated with it digital rights that results in such a classification. In any event, if the content is highly sensitive, process 500 branches to decision block 512; otherwise, process 500 proceeds to decision block 504.

[0061] At decision block 512, a determination is made whether the identifier provided by the remote device matches a pre-registered identifier associated with the remote device, and is the same as the identifier associated with the requested content. If the identifiers match, processing flows to decision block 508, described below; otherwise, processing flows to block 518, where access to the content is denied and the request is determined to be unauthorized.

[0062] Alternatively, at decision block 504, a determination is made whether the content is pre-determined as sensitive. Similarly, content may be pre-determined as sensitive employing a variety of mechanisms. In any event, if the content is sensitive, processing branches to decision block 514; otherwise processing continues to decision block 506.

[0063] At decision block 514, a determination is made whether a log-in associated with the content matches a log-in associated with the remote device. That is, in this embodiment, the end-user of the remote device is expected to log-in to the same account as is associated with the content. Such association may arise for example, when the content was originally provided to the server. In any event, if the log-ins do not match, the request is determined to be unauthorized and processing flows to block 518; otherwise, processing flows to decision block 506.

[0064] At decision block 506, a determination is made whether the content includes digital rights. If the content includes digital rights, processing branches to decision block 516; otherwise, processing continues to decision block 508.

[0065] At decision block 508, a determination is made whether a time period associated with content has expired. If the time period has expired, processing flows to block 518, where the request for access to the content is determined to be unauthorized (denied). Process 500 then returns to a calling process to perform other actions. However, if the time period is not expired, processing continues to block 510, where the request for the content is authenticated and authorized. Processing then returns to the calling process to perform other actions.

[0066] The present invention may further provide session continuity back to the client device from the remote device, as described in FIG. 6. Thus, FIG. 6 illustrates a logical flow diagram generally showing one embodiment of a process for providing action and/or content status to a client device using session continuity, in accordance with the present invention.

[0067] Process 600 of FIG. 6 begins, after a start block, at block 602, where a remote device having received content is enabled to perform an action on the received content. Such actions may include, for example, viewing the content, editing the content, deleting the content, forwarding the content to another device, associating the content into an application, file, text, and the like on the remote device, and
so forth. At least one of the actions performed on the remote device may affect a status of the content, such as a deletion, edit, viewing, and the like, may.

[0068] Processing next flows to block 604, where information about the action and/or the content status is sent towards the server. In one embodiment, the identifier associated with the remote device is also provided to the server. Processing continues to block 606, where the received identifier may be employed to update session data with the received action and/or content status information. Processing continues to block 608, where a client device, such as the client device originally providing the content may review the action and/or content status from the updated session data. Processing then returns to a calling process to perform other actions.

[0069] Processes 400, 500 and 600, then illustrate a continued session loop, from a client device to a remote device, and back to the client device.

[0070] It will be understood that each block of the flowchart illustrations discussed above, and combinations of blocks in the flowchart illustrations above, can be implemented by computer program instructions. These program instructions may be provided to a processor to produce a machine, such that the instructions, which execute on the processor, create means for implementing the actions specified in the flowchart block or blocks. The computer program instructions may be executed by a processor to cause a series of operational steps to be performed by the processor to produce a computer-implemented process such that the instructions, which execute on the processor, provide steps for implementing the actions specified in the flowchart block or blocks.

[0071] Accordingly, blocks of the flowchart illustration support combinations of means for performing the specified actions, combinations of steps for performing the specified actions and program instruction means for performing the specified actions. It will also be understood that each block of the flowchart illustration, and combinations of blocks in the flowchart illustration, can be implemented by special purpose hardware-based systems which perform the specified actions or steps, or combinations of special purpose hardware and computer instructions.

[0072] The above specification, examples, and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

What is claimed as new and desired to be protected by Letters Patent of the United States is:

1. A server for communicating content over a network, comprising:
   a transceiver for receiving and sending content over the network; and
   a content manager that is configured to perform actions, including:
   enabling a selection of content on a first computing device;
   receiving an identifier associated with a second computing device, wherein the first computing device and second computing device are currently uncoupled;
   receiving a request from the second computing device to access the server;
   receiving the identifier from the second computing device; and
   enabling access to the content by the second computing device based on the identifier, wherein the identifier further enables session continuity between the first computing device and the second computing device.
2. The server of claim 1, wherein the content manager is configured to perform actions, further comprising:
   receiving, from the second computing device, at least one of an action and a status associated with the content; and
   enabling access by the first computing device to the at least one action and status, using, in part, the identifier from the second computing device to further session continuity.
3. The server of claim 1, wherein enabling access to the content further comprises, authenticating the second computing device using, at least in part, the identifier.
4. The server of claim 1, wherein enabling access to the content further comprises, enabling access to the content if the second computing device is authorized to access the content.
5. The server of claim 1, wherein enabling access to the content further comprises, enabling access if a time period associated with the content is not expired.
6. The server of claim 1, wherein the second computing device is a mobile device.
7. The server of claim 1, wherein the content further comprises at least one of a graphic image, an audio file, a screen shot, a document, a binary file, a video file, a File Transfer Protocol command, a compressed file, a script, an application, an email message, and an alert.
8. The server of claim 1, wherein the identifier further comprises at least one of Mobile Identification Number (MIN), a Mobile Station International ISDN Number (MSISDN), Media Access Control (MAC) address, Internet Protocol (IP) address, and an electronic serial number (ESN).
9. The server of claim 1, wherein enabling access to the content further comprises employing at least one of a Short Message Service (SMS), Multimedia Message Service (MMS), instant messaging (IM), internet relay chat (IRC), mIRC, Jabber, and an HTTP protocol.
10. The server of claim 1, wherein the content manager performs actions further comprising storing the based, at least in part, on the identifier.
11. The server of claim 10, wherein the stored content is indexed using the identifier.
12. A method of communicating content over a network, comprising:
   enabling a selection of content on a first computing device;
   sending, by the first computing device, an identifier associated with a second computing device, wherein the first computing device and second computing device are currently uncoupled;
   sending a request from the second computing device to access a server;
sending the identifier from the second computing device to the server;

determining if the second computing device is authorized to access the content; and

if the second computing device is authorized, enabling access to the content by the second computing device based on the identifier.

13. The method of claim 12, wherein determining if the second computing device is authorized further comprises, authenticating the second computing device using, at least in part, the identifier from the second computing device.

14. The method of claim 12, wherein determining if the second computing device is authorized further comprises, determining a level of sensitivity associated with the content.

15. The method of claim 14, wherein determining a level of sensitivity further comprises, if the level of sensitivity is high, authenticating the second computing device based, at least in part, on a pre-registered identifier.

16. The method of claim 14, wherein determining a level of sensitivity further comprises, if the level of sensitivity is moderate, authenticating the second computing device based, at least in part, on if the second computing device is logged into a same account as the first computing device was when sending the identifier associated with the second computing device.

17. The method of claim 12, wherein the second computing device is a mobile device.

18. The method of claim 12, wherein the content further comprises at least one of a graphic image, an audio file, a screen shot, a document, a binary file, a video file, a File Transfer Protocol command, a compressed file, a script, an application, an email message, and an alert.

19. The method of claim 12, wherein the identifier further comprises at least one of Mobile Identification Number (MIN), a Mobile Station International ISDN Number (MSISDN), Media Access Control (MAC) address, Internet Protocol (IP) address, and an electronic serial number (ESN).

20. The method of claim 12, wherein enabling access to the content further comprises employing an asynchronous message protocol.

21. The method of claim 12, wherein enabling access to the content further comprises employing a message hook, including at least one of a Uniform Resource Locator (URL), the identifier, a script, and an executable program.

22. The method of claim 12, where enabling the selection further comprises providing at least one of a toolbar button, an icon, a script, a link, a drop-down menu, a pop-up menu, and an application for use in selecting the content.

23. The method of claim 12, wherein enabling access to the content further comprises employing at least one of a Short Message Service (SMS), Multimedia Message Service (MMS), instant messaging (IM), internet relay chat (IRC), Jabber, and an HTTP protocol.

24. A modulated data signal for communicating content over a network, the modulated data signal comprising:

- enabling a selection of content on a first computing device;

- sending from the first computing device an identifier associated with a second computing device, wherein the first computing device and second computing device are currently uncoupled;

- sending a request from the second computing device to access the server;

- sending the identifier from the second computing device; and

if the second computing device is authorized, enabling access to the content by the second computing device based on the identifier.

25. The modulated data signal of claim 24, wherein the second computing device is a mobile device.

26. The modulated data signal of claim 24, wherein if the second computing device is authorized further comprises, determining authorization based one at least one of a sensitivity associated with the content, a digital right associated with the content, and a time period associated with the content.

27. The modulated data signal of claim 24, wherein the content further comprises at least one of a graphic image, an audio file, a screen shot, a document, a binary file, a video file, a File Transfer Protocol command, a compressed file, a script, an application, an email message, and an alert.

28. The modulated data signal of claim 24, wherein the identifier further comprises at least one of Mobile Identification Number (MIN), a Mobile Station International ISDN Number (MSISDN), Media Access Control (MAC) address, Internet Protocol (IP) address, and an electronic serial number (ESN).

29. A server for communicating content over a network, comprising:

- a transceiver for receiving and sending content over the network; and

- a content manager that is configured to perform actions, including:

  - a means for enabling a selection of content on a first computing device;

  - a means for receiving an identifier associated with a second computing device, wherein the first computing device and second computing device are currently uncoupled;

  - a means for employing the identifier to store the content;

  - a means for receiving a request from the second computing device to access the server;

  - a means for receiving the identifier from the second computing device;

  - a means for employing the identifier to retrieve the stored content; and

  - a means for providing the content to the second computing device, wherein the identifier enables session continuity between the first computing device and the second computing device.

* * * * *