US 20120117478A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2012/0117478 A1

(43) Pub. Date: May 10, 2012

Vadde et al.

(54) MANAGING NETWORK USAGE PER APPLICATION VIA POLICIES

(75) Inventors: **Kiran Kumar Vadde**, Sammamish, WA (US); **Kevin A. Chin**, Bellevue, WA (US); **Harish Srinivasan**, Sammamish, WA (US); **Omar M. Maabreh**, Bellevue, WA (US)

(73) Assignee: **MICROSOFT CORPORATION**, Redmond, WA (US)

(21) Appl. No.: **12/942,423**

(22) Filed: **Nov. 9, 2010**

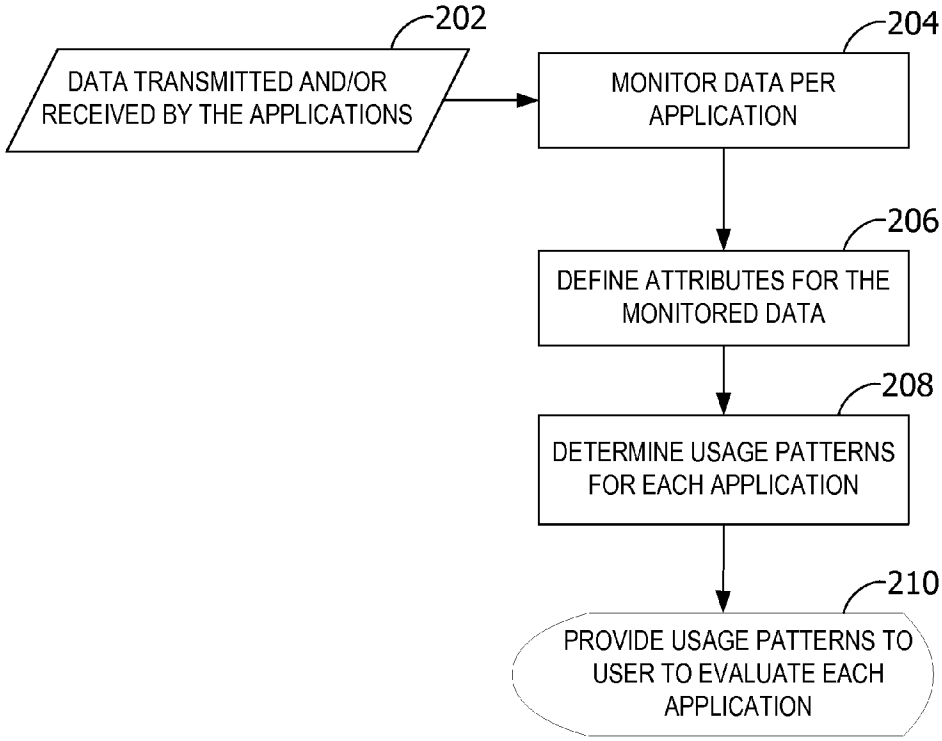
Publication Classification

(51) **Int. Cl.**
G06F 15/16 (2006.01)
G06F 3/01 (2006.01)

(52) **U.S. Cl.** **715/736**; 709/224

(57) **ABSTRACT**

Defining and applying policies to manage data traffic including data transmitted and/or received by each of a plurality of applications executing on a computing device. The data traffic is monitored per application and attributes are defined for the monitored data traffic to enable the user to evaluate the data traffic for each application. Usage patterns are determined based on the monitored data traffic and the attributes to create one or more policies. The policies are applied to prevent each application from exceeding a corresponding data usage limit defined by the policies.



GOOGLE EXHIBIT 1042

FIG. 1

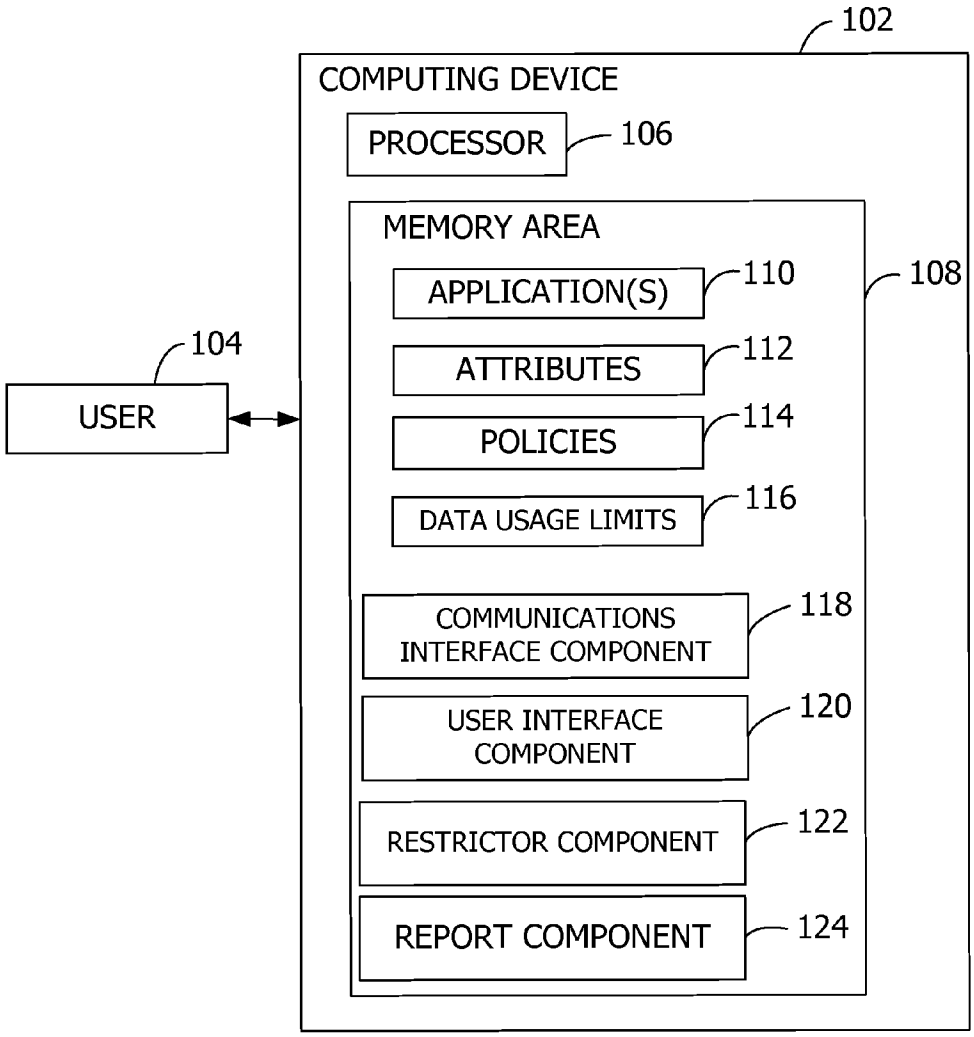

102
COMPUTING DEVICE
PROCESSOR
106
MEMORY AREA
108
APPLICATION(S)
110
ATTRIBUTES
112
POLICIES
114
DATA USAGE LIMITS
116
104
USER
COMMUNICATIONS INTERFACE COMPONENT
118
USER INTERFACE COMPONENT
120
RESTRICTOR COMPONENT
122
REPORT COMPONENT
124

FIG. 2

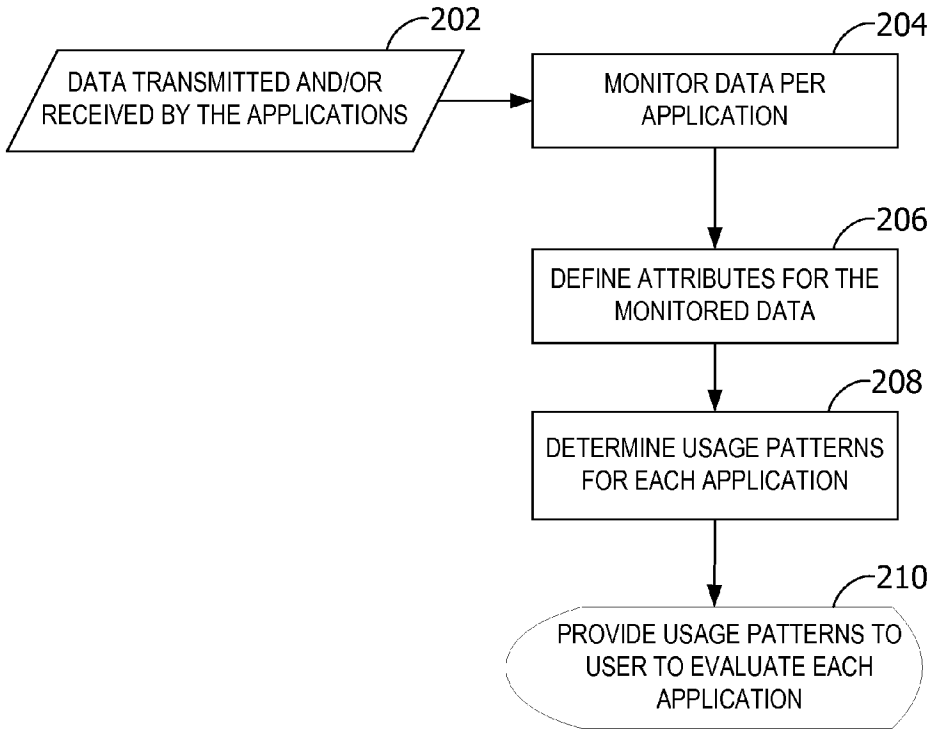
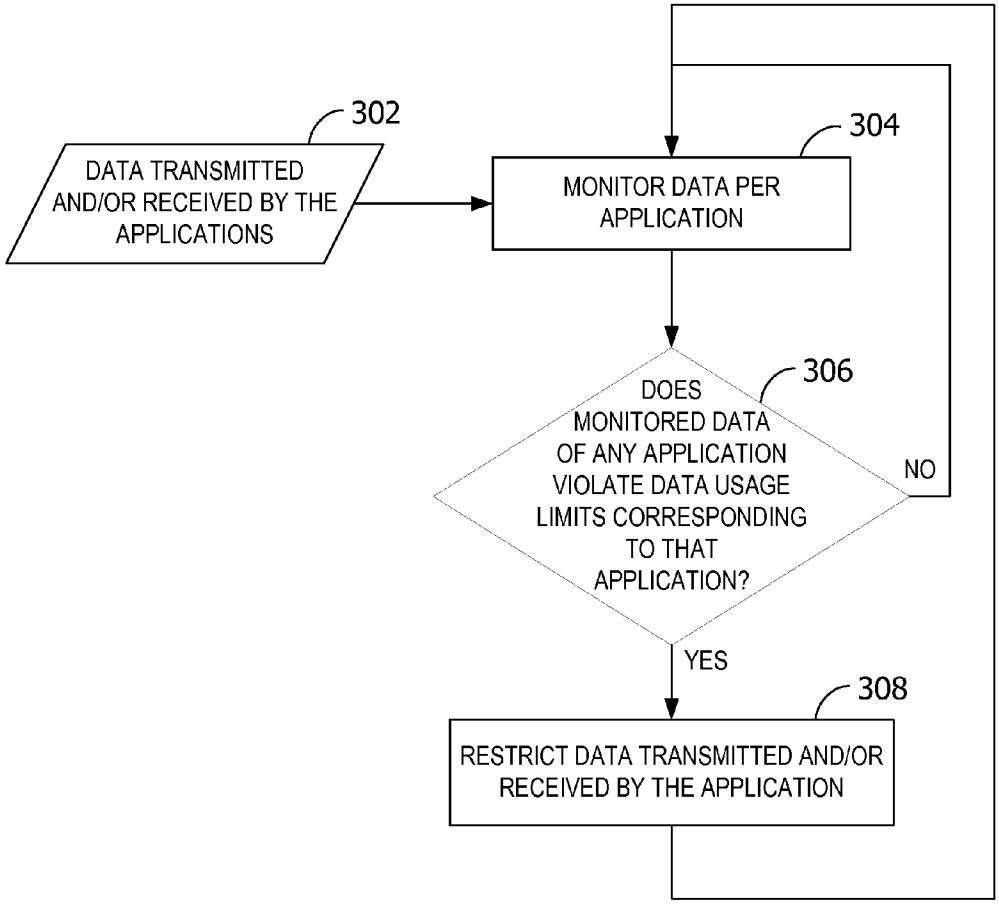

202
DATA TRANSMITTED AND/OR RECEIVED BY THE APPLICATIONS
204
MONITOR DATA PER APPLICATION
206
DEFINE ATTRIBUTES FOR THE MONITORED DATA
208
DETERMINE USAGE PATTERNS FOR EACH APPLICATION
210
PROVIDE USAGE PATTERNS TO USER TO EVALUATE EACH APPLICATION

FIG. 3


302
DATA TRANSMITTED AND/OR RECEIVED BY THE APPLICATIONS
304
MONITOR DATA PER APPLICATION
306
DOES MONITORED DATA OF ANY APPLICATION VIOLATE DATA USAGE LIMITS CORRESPONDING TO THAT APPLICATION?
NO
YES
308
RESTRICT DATA TRANSMITTED AND/OR RECEIVED BY THE APPLICATION

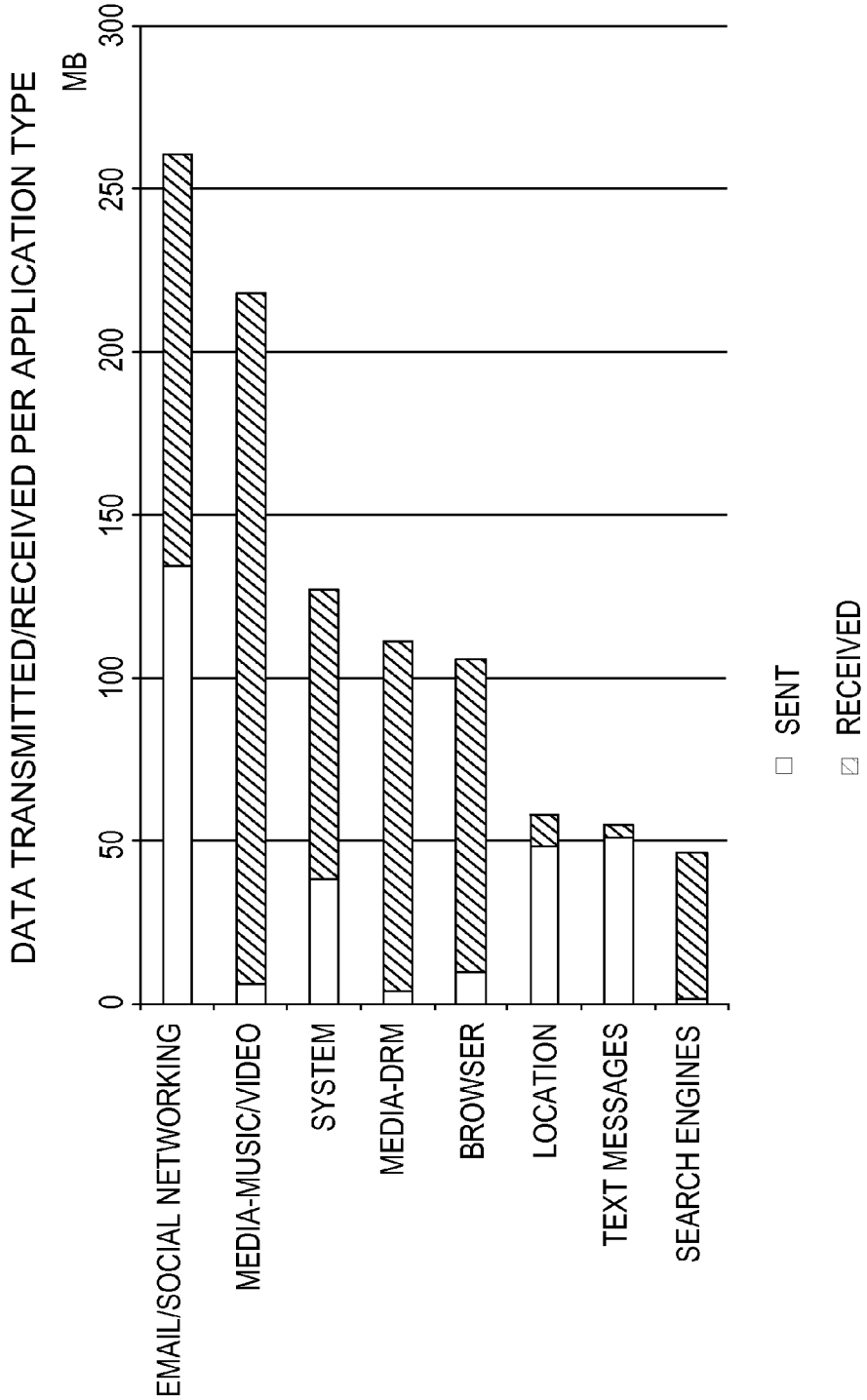

DATA TRANSMITTED/RECEIVED PER APPLICATION TYPE
MB
0
50
100
150
200
250
300
EMAIL/SOCIAL NETWORKING
MEDIA-MUSIC/VIDEO
SYSTEM
MEDIA-DRM
BROWSER
LOCATION
TEXT MESSAGES
SEARCH ENGINES
SENT
RECEIVED

FIG. 4

MANAGING NETWORK USAGE PER APPLICATION VIA POLICIES

BACKGROUND

[0001] The cost of mobile operator data plans is often based on usage. Each data plan has data usage limits, but users have difficulty determining when the data usage limits have been reached or are about to be reached with existing systems. As a result, users can incur excess data charges. Further, with existing systems, users are unable to determine the relative costs incurred by different applications executing on a mobile telephone.

SUMMARY

[0002] Embodiments of the disclosure manage data traffic per application. Data transmitted and/or received by each of a plurality of applications executing on a computing device is monitored. One or more attributes associated with the monitored data are defined for each of the plurality of applications. Usage patterns for each of the plurality of applications are determined based at least on the monitored data and the defined attributes associated therewith. The determined usage patterns are provided to a user of the computing device for evaluation of each of the plurality of applications.

[0003] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. **1** is an exemplary block diagram illustrating a computing device storing policies for enforcing data usage limits of applications.

[0005] FIG. **2** is an exemplary flow chart illustrating operation of the computing device to monitor data transmitted and/or received by applications executing on the computing device and to develop usage patterns based thereon.

[0006] FIG. **3** is an exemplary flow chart illustrating operation of the computing device to restrict data transmitted and/or received by applications executing on the computing device.

[0007] FIG. **4** is an exemplary diagram illustrating data transmitted and received per application type.

[0008] Corresponding reference characters indicate corresponding parts throughout the drawings.

DETAILED DESCRIPTION

[0009] Referring to the figures, embodiments of the disclosure enable data budgets to be invoked per application **110**. In some embodiments, data traffic is monitored per application **110** along with attributes **112** such as time of day, location, type of network interface, and amount of data during an interval (e.g., month). Sample network interface types include cellular, wireless fidelity (WiFi), and the like. Usage patterns are developed that form the basis of policies **114** that are used to restrict data traffic per application **110** over specific networks, locations, times, and the like. The policies **114** may also be used to reduce battery usage, mobile operator charges, and/or processor usage by restricting data traffic. Further, aspects of the disclosure enable users **104** to save money on their monthly network operator bill (e.g., wireless bill).

[0010] Referring again to FIG. **1**, an exemplary block diagram illustrates a computing device **102** storing policies **114** for enforcing data usage limits **116** of applications **110**. In the example of FIG. **1**, the computing device **102** associated with the user **104** represents a system for managing data traffic per application **110**. The computing device **102** represents any device executing instructions (e.g., as application programs, operating system functionality, or both) to implement the operations and functionality associated with the computing device **102**. The computing device **102** may include a mobile computing device or any other portable device. In some embodiments, the mobile computing device includes a mobile telephone, laptop, netbook, gaming device, and/or portable media player. The computing device **102** may also include less portable devices such as desktop personal computers, kiosks, and tabletop devices. Additionally, the computing device **102** may represent a group of processing units or other computing devices.

[0011] The computing device **102** has at least one processor **106** and a memory area **108**. The processor **106** includes any quantity of processing units, and is programmed to execute computer-executable instructions for implementing aspects of the disclosure. The instructions may be performed by the processor **106** or by multiple processors executing within the computing device **102**, or performed by a processor external to the computing device **102**. In some embodiments, the processor **106** is programmed to execute instructions such as those illustrated in the figures (e.g., FIG. **2** and FIG. **3**).

[0012] The computing device **102** further has one or more computer-readable media such as the memory area **108**. The memory area **108** includes any quantity of media associated with or accessible by the computing device **102**. The memory area **108** may be internal to the computing device **102** (as shown in FIG. **1**), external to the computing device **102** (not shown), or both (not shown).

[0013] The memory area **108** stores, among other data, one or more applications **110**. The applications **110**, when executed by the processor **106**, operate to perform functionality on the computing device **102**. Exemplary applications **110** include mail application programs, web browsers, calendar application programs, address book application programs, messaging programs, media applications, location-based services, search programs, and the like. The applications **110** may communicate with counterpart applications or services such as web services accessible via a network. For example, the applications **110** may represent downloaded client-side applications that correspond to server-side services executing in a cloud.

[0014] The memory area **108** further stores one or more attributes **112**, policies **114**, and data usage limits **116**. As further described below, the attributes **112** represent characteristics of, or otherwise describe, data that is transmitted or received by the applications **110**. Each of the applications **110** has a set of attributes **112** corresponding thereto. Exemplary attributes **112** include, but are not limited to, a transmission time, receipt time, duration, network interface type, port, location of the computing device **102**, network operator, quantity of data sent, quantity of data received, application name, or permissions.

[0015] The policies **114** represent rules, limitations, qualifications, or other criteria for managing data transmitted and/

or received by the applications **110**. As further described below, the policies **114** are defined based on a plurality of inputs such as the attributes **112** and the data transmitted and/or received by the applications **110**, and may apply to one or more of the applications **110**.

[0016] The data usage limits **116** place restrictions on the quantity and/or type of data transmitted and/or received by each of the applications **110**. In some embodiments, each of the applications **110** has one or more of the data usage limits **116** corresponding thereto.

[0017] The memory area **108** further stores one or more computer-executable components. Exemplary components include a communications interface component **118**, a user interface component **120**, a restrictor component **122**, and a report component **124**. The communications interface component **118**, when executed by the processor **106** of the computing device **102**, causes the processor **106** to provide a profile of the user **104** of the computing device **102** (e.g., a first computing device) to another computing device (e.g., a second computing device). The profile describes the user **104** and/or the first computing device, and may include, for example, a list of installed applications **110**, operating system version, corporate affiliation (e.g., employment of the user **104**), explicit preferences of the user **104**, inferred preferences of the user **104**, user activity history (e.g., browsing history, interaction with the first computing device), and the like.

[0018] The second computing device represents, for example, a server or other remote device that communicates with a plurality of first computing devices (such as computing device **102**). The second computing device maintains, or has access to, a plurality of policies **114** such as data usage policies. In some embodiments, the second computing device collects the data usage policies (or usage patterns) from the plurality of first computing devices, and acts as a central repository to aggregate the data usage policies (or usage patterns). For example, the first computing devices create and share the data usage policies with the second computing device. In some embodiments, based on the received profile of the user **104**, the second computing device selects one or more data usage policies. In this manner, users **104** with similar usage habits share the same data usage policies. Each of the data usage policies includes data usage limits **116**. Each of the data usage limits **116** corresponds to at least one of the applications **110** executing on the first computing device. Alternatively or in addition, the data usage limits **116** correspond to application types (e.g., browser, email, search, location, etc.).

[0019] The communications interface component **118** further executes on the first computing device to receive the selected data usage policies from the second computing device. In some embodiments, the communications interface component **118** includes a network interface card and/or computer-executable instructions (e.g., a driver) for operating the network interface card.

[0020] The user interface component **120**, when executed by the processor **106**, causes the processor **106** to provide the data usage policies received by the communications interface component **118** to the user **104**. For example, a list of the received data usage policies may be displayed to the user **104**. The user interface component **120** further executes to receive from the user **104** a selection of at least one of the provided data usage policies. In some embodiments, the user **104** selects multiple data usage policies, and assigns each selected data usage policy to one or more of the applications **110**. The user **104** may also identify applications **110** to which none of the data usage policies applies. In such embodiments, the identified applications **110** represent an exception list.

[0021] In some embodiments, the user interface component **120** includes a graphics card for displaying data to the user **104** and receiving data from the user **104**. The user interface component **120** may also include computer-executable instructions (e.g., a driver) for operating the graphics card. Further, the user interface component **120** may include a display (e.g., a touch screen display) and/or computer-executable instructions (e.g., a driver) for operating the display. The user interface component **120** may also include one or more of the following to provide data to the user **104** or receive data from the user **104**: speakers, a sound card, a camera, a microphone, a vibration motor, and one or more accelerometers. For example, the user **104** may input commands or manipulate data by moving the computing device **102** in a particular way.

[0022] The restrictor component **122**, when executed by the processor **106**, causes the processor **106** to apply the data usage policy selected by the user **104** via the user interface component **120** to one or more of the applications **110** executing on the first computing device. Applying the data usage policy prevents the applications **110** from transmitting and/or receiving data in excess of the data usage limits **116** associated with the applied data usage policy. Applying the data usage policy includes determining whether any of the criteria in the data usage policy has been violated. For example, the restrictor component **122** monitors the data transmitted and/or received by the applications **110** and determines whether the data usage limits **116** corresponding to each of the applications **110** have been exceeded or are about to be exceeded (e.g., within a percentage such as 80% of the maximum or absolute threshold). In some embodiments, the restrictor component **122** monitors the data by receiving or accessing the attributes **112** or other statistics describing the data transmitted and/or received by each of the applications **110**.

[0023] The report component **124**, when executed by the processor **106**, causes the processor **106** to provide the user **104** with a data cost associated with each of the applications **110**. The data cost is derived by correlating the amount and/or type of data traffic with a cost for handling the data traffic. The cost may be a financial cost that is set, for example, by a network operator (e.g., a mobile operator). Other costs are contemplated and include, for example, a resource cost corresponding to an amount of battery power consumed when handling the data traffic. In some embodiments, the report component **124** produces data (e.g., in chart form) that shows the data cost per application **110**.

[0024] Referring next to FIG. **2**, an exemplary flow chart illustrates operation of the computing device **102** to monitor data transmitted and/or received by applications **110** executing on the computing device **102** and to develop usage patterns based thereon. At **202**, data is transmitted and/or received by the applications **110**. At **204**, aspects of the disclosure monitor the data to define, at **206**, one or more of the attributes **112**. Exemplary attributes **112** include, but are not limited to, a transmission time, receipt time, duration, network interface type, network destination, device battery status, port, location of the computing device **102**, network operator, quantity of data sent, quantity of data received, application name, or permissions. In some embodiments, each of the applications **110** has a corresponding set of

attribute values. At **208**, usage patterns are determined for each of the applications **110**. The usage patterns are determined based at least on the monitored data and the defined attributes **112**. For example, the usage patterns may identify patterns in the volume and type of data transmitted and/or received, the type of network interface used, times during the day for heavy and light volume, and the like. At **210**, the determined usage patterns are provided to the user **104** of the computing device **102**. The user **104** analyzes or evaluates each application **110** based on the usage pattern corresponding to that application **110**. For example, the usage patterns may be grouped per application **110** such that the user **104** is able to evaluate each of the applications **110** based on the associated usage pattern. In another example, the usage patterns are grouped per attribute **112** such that the user **104** is able to compare each of the applications **110** based on the attribute **112** (e.g., which application **110** uses the cellular radio the most, which application **110** uses a WiFi network adapter the most, etc.).

[0025] Aspects of the disclosure may further operate to receive, from the user **104**, the data usage limits **116** associated with each of the applications **110**. For example, the user **104** may specify a maximum quantity of data to be transmitted and/or received by a particular application **110**. The user **104** may also specify the quantity per other attributes **112** such as per time interval (e.g., during peak or business hours versus off-peak or weekend and night hours), per network interface type, or per location of the computing device **102**.

[0026] In some embodiments, the policies **114** are created based on the defined attributes **112**, the received data usage limits **116**, user preferences, system preferences, and/or other criteria. Aspects of the disclosure apply the policies **114** to prevent the applications **110** from violating the data usage limits **116** (e.g., exceeding a maximum data usage). The policies **114** apply to one or more of the applications **110**. In some embodiments, the policies **114** prioritize a first one of the applications **110** over a second one of the applications **110** such that if remaining data usage is limited, the first application is given priority over the second application to use the remaining data usage. In such embodiments, the data traffic of the second application is restricted, as described below with reference to FIG. **3**.

[0027] Aspects of the disclosure may further receive, from the user **104**, an assignment of at least one of the applications **110** to at least one of a plurality of categories. Example categories include business, leisure, recreation, personal, and private. For example, the business category may include electronic mail programs and calendar programs, while the leisure category may include social networking applications and games. In such embodiments, the usage patterns may be grouped by category such that the user **104** is able to evaluate the data traffic used by each category of the applications **110**.

[0028] In some embodiments, recommendations may be given based on the determined usage patterns. The recommendation may be provided to the user **104** along with the usage patterns. For example, if aspects of the disclosure determine that a particular program or category of programs is generated an excessive amount of data traffic, that program or category may be identified for deletion. The user **104** is prompted to accept or reject the recommendation.

[0029] Referring next to FIG. **3**, an exemplary flow chart illustrates operation of the computing device **102** to restrict data transmitted and/or received by applications **110** executing on the computing device **102**. At **302**, data is transmitted and/or received by the applications **110**. At **304**, aspects of the disclosure monitor the transmitted and/or received data per application **110**. At **306**, the monitored data of each application **110** is compared with the corresponding data usage limits **116** for that application **110** to determine whether the data usage limits **116** have been violated (or are about to be violated). If no violation or trigger has occurred, the data continues to be monitored at **304**. If a violation or trigger has occurred, the application **110** associated with the violation is restricted from transmitting and/or receiving additional data. For example, limits may be placed on how much data may be transmitted and/or received during certain periods of the day (e.g., during peak hours). In another example, the application **110** may be automatically blocked from transmitting and/or receiving any data (e.g., download of a web page may be halted when the threshold is reached). In still another example, the user **104** is prompted to manually consent to or reject a recommendation to restrict the data traffic of a particular application **110**.

[0030] While the restriction at **308** affects the application **110** deemed to be in violation of the data usage limits **116**, other applications **110** may continue to transmit and/or receive data. As such, the monitoring continues at **304**.

[0031] Referring next to FIG. **4**, an exemplary diagram illustrates data transmitted and received per application type. The values represented by the diagram are generated by aspects of the disclosure (e.g., the report component **124**). In the example of FIG. **4**, the vertical axis lists the application types including email/social networking applications, multimedia applications, operating system applications, digital rights management applications, browsers, applications using location-based services, text messaging applications, and search engines. The horizontal axis represents the total quantity of data traffic sent and/or received by each type or category of application **110**. The cross-hatching indicates the division between the amount of data sent versus the amount of data received by each type of application **110**.

Additional Examples

[0032] Listed below is an example policy designed for users in a corporate environment. The example policy considers applications in use, roaming status, byte budgets (e.g., by percentage and absolute), and network interface types. The example policy also provides criteria for prompting the user to override restrictions as budgets are approached.

```
<budget>
    <policy Cellular>
        <Program ID=EMAIL, Limit=500MB, Send=100MB,
Roaming=YES>
        <Program ID=SocialNetworkingSiteA, Limit=10MB>
        <Program ID=DEF, Limit=10MB, Roaming=NO>
        <PromptReminder Criteria=Bytes, PercentofBudget=50%>
        <PromptData Criteria=Bytes, PercentofBudget=90%>
        <PromptData Criteria=Roaming, Limit=20MB>
    </policy>
    <policy WiFi>
        <Program ID=XYZ, Limit=5000MB>
        <Program ID=ABC, Limit=5000MB>
    </policy>
</budget>
```

[0033] In an example scenario, an employee is provided with an employer-sponsored mobile telephone. At the time of configuration, a corporate usage policy may be installed to ensure that the mobile operator costs will be in line with employer policy. There may be different policies **114** for different employees based on the level of the employee, type of mobile telephone, and level of sponsorship. The data usage limits **116** may appear as reminders to the employee or may be more automatically restrictive based on allowable budget.

[0034] In another example, the user is about to visit another country but is concerned about roaming network charges. A policy may be generated based on her home mobile operator, employer, peer group, or other context. The policy is based on financial amounts and applications or types of applications the user plans to use while roaming. For example, web search engines and location-based service may be able to send and/or receive data without data usage limits **116** up to a predefined maximum financial amount (e.g., $50). In contrast, social networking applications are only able to send and/or receive data using a WiFi network connection to ensure that costs are not accidentally incurred while roaming.

[0035] In still another example, a salesperson on commission wants to track the business-related costs of using a mobile telephone. Using aspects of the disclosure, the salesperson can identify the quantity of data sent and/or received by business applications. The salesperson is then able to bill an employer for that identified quantity. The salesperson is also able to identify which personal or leisure applications are incurring costs during working hours. On the employer side, the employer can access aspects of the invention to confirm the identified quantity of data based on centralized monitoring of the data traffic.

[0036] At least a portion of the functionality of the various elements in FIG. **1** may be performed by other elements in FIG. **1**, or an entity (e.g., processor, web service, server, application program, computing device, etc.) not shown in FIG. **1**.

[0037] In some embodiments, the operations illustrated in FIG. **2** and FIG. **3** may be implemented as software instructions encoded on a computer-readable medium, in hardware programmed or designed to perform the operations, or both. For example, aspects of the disclosure may be implemented as a system on a chip.

[0038] While no personally identifiable information is tracked by aspects of the disclosure, embodiments have been described with reference to data monitored and/or collected from users **104**. In such embodiments, notice is provided to the users **104** of the collection of the data (e.g., via a dialog box or preference setting) and users **104** are given the opportunity to give or deny consent for the monitoring and/or collection. The consent may take the form of opt-in consent or opt-out consent.

Exemplary Operating Environment

[0039] Exemplary computer readable media include flash memory drives, digital versatile discs (DVDs), compact discs (CDs), floppy disks, and tape cassettes. By way of example and not limitation, computer readable media comprise computer storage media and communication media. Computer storage media store information such as computer readable instructions, data structures, program modules or other data. Communication media typically embody computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and include any information delivery media. Combinations of any of the above are also included within the scope of computer readable media.

[0040] Although described in connection with an exemplary computing system environment, embodiments of the invention are operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with aspects of the invention include, but are not limited to, mobile computing devices, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, gaming consoles, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0041] Embodiments of the invention may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. The computer-executable instructions may be organized into one or more computer-executable components or modules. Generally, program modules include, but are not limited to, routines, programs, objects, components, and data structures that perform particular tasks or implement particular abstract data types. Aspects of the invention may be implemented with any number and organization of such components or modules. For example, aspects of the invention are not limited to the specific computer-executable instructions or the specific components or modules illustrated in the figures and described herein. Other embodiments of the invention may include different computer-executable instructions or components having more or less functionality than illustrated and described herein.

[0042] Aspects of the invention transform a general-purpose computer into a special-purpose computing device when configured to execute the instructions described herein.

[0043] The embodiments illustrated and described herein as well as embodiments not specifically described herein but within the scope of aspects of the invention constitute exemplary means for determining a quantity of data transmitted and/or received by each of the plurality of applications **110**, and exemplary means for defining and applying a policy **114** for managing data traffic per application **110**.

[0044] The order of execution or performance of the operations in embodiments of the invention illustrated and described herein is not essential, unless otherwise specified. That is, the operations may be performed in any order, unless otherwise specified, and embodiments of the invention may include additional or fewer operations than those disclosed herein. For example, it is contemplated that executing or performing a particular operation before, contemporaneously with, or after another operation is within the scope of aspects of the invention.

[0045] When introducing elements of aspects of the invention or the embodiments thereof, the articles "a," "an," "the," and "said" are intended to mean that there are one or more of the elements. The terms "comprising," "including," and "having" are intended to be inclusive and mean that there may be additional elements other than the listed elements.

[0046] Having described aspects of the invention in detail, it will be apparent that modifications and variations are possible without departing from the scope of aspects of the invention as defined in the appended claims. As various changes could be made in the above constructions, products, and methods without departing from the scope of aspects of the invention, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

What is claimed is:

1. A system for managing data traffic per application, said system comprising:

a memory area associated with a mobile computing device, said memory area storing data usage limits corresponding to each of a plurality of applications executed by the mobile computing device;

a processor programmed to:

monitor data transmitted and/or received by each of the plurality of applications;

compare the monitored data with the corresponding data usage limits stored in the memory area; and

restrict data transmitted and/or received by each of the applications based on the comparison.

2. The system of claim **1**, wherein the processor is programmed to restrict the data by halting download of a web page by the mobile computing device.

3. The system of claim **1**, wherein the processor is programmed to receive the data usage limits for storage in the memory area.

4. The system of claim **1**, wherein the processor is further programmed to prompt, when the monitored data exceeds the corresponding data usage limit for one of the applications, a user of the mobile computing device for consent to restrict data transmitted and/or received by said one of the applications.

5. The system of claim **1**, further comprising means for determining a quantity of data transmitted and/or received by each of the plurality of applications.

6. The system of claim **1**, further comprising means for defining and applying a policy for managing data traffic per application.

7. A method comprising:

monitoring data transmitted and/or received by each of a plurality of applications executing on a computing device;

defining one or more attributes associated with the monitored data for each of the plurality of applications;

determining usage patterns for each of the plurality of applications based at least on the monitored data and the defined attributes associated therewith; and

providing the determined usage patterns to a user of the computing device for evaluation of each of the plurality of applications.

8. The method of claim **7**, further comprising:

receiving, from the user, data usage limits associated with each of the plurality of applications;

defining a policy based on the defined attributes and the received data usage limits; and

applying the defined policy to prevent each of the plurality of applications from exceeding the received data usage limits associated therewith.

9. The method of claim **8**, wherein the defined policy prioritizes a first one of the applications over a second one of the applications for data transmitted and/or received.

10. The method of claim **8**, further comprising providing the defined policy to another computing device, wherein the other computing device applies the defined policy to applications executing on the other computing device.

11. The method of claim **7**, wherein defining the one or more attributes comprises defining one or more of the following: transmission time, receipt time, duration, network interface type, port, location of the computing device, network operator, quantity of data sent, quantity of data received, application name, and permissions.

12. The method of claim **7**, wherein providing the determined usage patterns to the user comprises providing the determined usage patterns grouped per application, wherein the user evaluates each of the applications based on the determined usage patterns associated therewith.

13. The method of claim **7**, wherein providing the determined usage patterns to the user comprises providing the determined usage patterns grouped per defined attribute, wherein the user evaluates each of the applications based on the defined attribute.

14. The method of claim **7**, further comprising receiving, from the user, an assignment of one or more of the plurality of applications to at least one of a plurality of categories, wherein determining the usage patterns comprises determining usage patterns for the categories, and wherein the user evaluates the categories based on the determined usage patterns.

15. The method of claim **14**, wherein receiving the assignment comprises receiving an assignment of one or more of the plurality of applications to one or more of the following categories: business, leisure, recreation, personal, and private.

16. The method of claim **7**, further comprising recommending deletion of at least one of the applications based on the determined usage patterns.

17. One or more computer-readable media having computer-executable components, said components comprising:

a communications interface component that when executed by at least one processor of a first computing device causes the at least one processor to:

provide a profile of a user of the first computing device to a second computing device, and

receive one or more data usage policies from the second computing device, wherein the second computing device selects the one or more data usage policies based on the profile of the user, wherein each of the data usage policies have data usage limits each corresponding to at least one of a plurality of applications executing on the first computing device;

a user interface component that when executed by at least one processor of the first computing device causes the at least one processor to:

provide the data usage policies received by the communications interface component to the user, and

receive from the user a selection of at least one of the provided data usage policies; and

a restrictor component that when executed by at least one processor of the first computing device causes the at least one processor to apply the data usage policy selected by the user via the user interface component to one or more of the applications executing on the first computing device, wherein applying the data usage policy prevents the applications from transmitting and/or receiving data in excess of the data usage limits associated with the applied data usage policy.

18. The computer-readable media of claim **17**, wherein the restrictor component executes to apply the data usage policy by restricting data transmitted and/or received by at least one of the applications if the data usage limits for said at least one of the applications have been exceeded.

19. The computer-readable media of claim **17**, wherein the user interface component further executes to receive, from the user, an exception list of applications to which the data usage policies do not apply.

20. The computer-readable media of claim **17**, further comprising a report component that when executed by at least one processor of the first computing device causes the at least one processor to provide the user with a data cost associated with each of the applications.

* * * * *