(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102124487 A
(43)申请公布日 2011.07.13

(21)申请号 200980132570.3

(22)申请日 2009.08.14

(30)优先权数据
12/193,587 2008.08.18 US

(85)PCT申请进入国家阶段日
2011.02.17

(86)PCT申请的申请数据
PCT/US2009/053851 2009.08.14

(87)PCT申请的公布数据
WO2010/021926 EN 2010.02.25

(71)申请人 微软公司
地址 美国华盛顿州

(72)发明人 A·蔡格勒 A·P·盖加姆
M·B·帕顿 J·A·希契考克
D·J·阿查莫维奇 A·T·佐

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 黄嵩泉

(51)Int.Cl.
G06Q 50/00(2006.01)

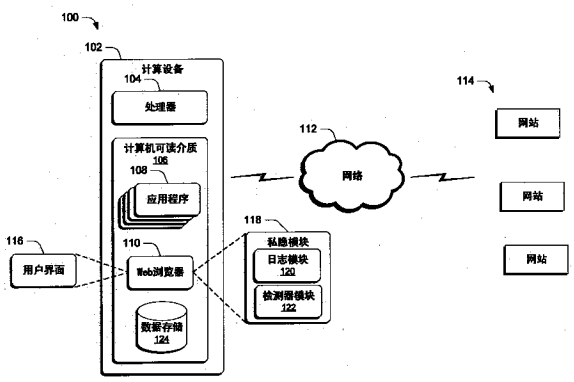
权利要求书 2 页 说明书 9 页 附图 6 页

(54)发明名称

网页私隐风险检测

(57)摘要

各实施例能够实现对可能引起对用户的私隐风险的第三方内容源的检测。在至少某些实施例中，可以处理经由浏览器导航到的网页来标识为网页提供内容的第三方内容源。可以存储将第三方内容源与其中遭遇该第三方内容的网页进行相关的数据。随后可以分析该数据来确定特定第三方何时处于可以观察用户的浏览习惯的位置。响应于确定了私隐风险，可以用各种方式来输出通知以向用户通知潜在危险的内容。在至少某些其他实施例中，通知可以经由自动呈现给用户的用户界面工具来作出以向用户通知潜在危险的第三方内容源。



CN 102124487 A

1. 一种计算机实现的方法，包括：

接收与网页相关联的 HTML 代码；

处理所述 HTML 代码来标识为所述网页提供内容的一个或多个第三方；

对于个体所标识的第三方，存储将第三方与所述第三方为其提供内容的一个或多个网页进行相关的数据；

根据关于特定第三方存储的数据来检测所述特定第三方是否处于可以观察用户的浏览习惯的位置；以及

响应于所述检测，输出能使得所述用户能够关于来自所述特定第三方的内容采取一个或多个动作的用户界面工具。

2. 如权利要求 1 所述的计算机实现的方法，其特征在于，所述检测和输出由 Web 浏览器来执行。

3. 如权利要求 1 所述的计算机实现的方法，其特征在于，所述用户界面工具包括弹出窗口。

4. 如权利要求 1 所述的计算机实现的方法，其特征在于，所述用户界面工具包括使得所述用户能够提供输入来指定是阻塞还是允许所述内容的一个或多个可选按钮。

5. 如权利要求 1 所述的计算机实现的方法，其特征在于，所述用户界面工具包括使得所述用户能够获得关于所述特定第三方的附加信息的可选链接。

6. 如权利要求 5 所述的计算机实现的方法，其特征在于，所述可选链接在被选择时导致重定向到所述特定第三方的网站来使得所述用户能够从所述特定第三方获得所述附加信息。

7. 如权利要求 1 所述的计算机实现的方法，其特征在于，所述检测包括每一次所述特定第三方与不同的网页相关时递增与所述特定第三方相关联的计数器。

8. 如权利要求 1 所述的计算机实现的方法，其特征在于，还包括：

经由所述用户界面工具从所述用户接收输入；以及

根据来自所述用户的输入阻塞或允许来自所述特定第三方的内容。

9. 一种计算机实现的方法，包括：

接收与网页相关联的 HTML 代码；

处理所述 HTML 代码来标识要被包括在所述网页中的来自第三方内容源的内容；

计算在由应用程序导航到的网页中遭遇来自所述第三方内容源的内容的次数；

基于所计算的次数，查明所述第三方内容源是否处于可以观察所述应用程序的用户的浏览习惯的位置。

10. 如权利要求 0 所述的计算机实现的方法，其特征在于，还包括响应于所述查明，输出用户界面工具来向用户通知所检测的第三方内容源。

11. 如权利要求 10 所述的计算机实现的方法，其特征在于，还包括：

基于所计算的次数将感觉到的风险级别指派给第三方内容源；以及

经由所述用户界面工具输出来呈现所感觉到的风险级别以向所述用户通知所检测的第三方内容源。

12. 如权利要求 10 所述的计算机实现的方法，其特征在于，所述用户界面工具采用出现在所述应用程序的菜单栏中的菜单栏项的形式。

13. 如权利要求 0 所述的计算机实现的方法，其特征在于，还包括响应于所述查明，输出具有使得所述用户能够关于所检测的第三方内容源采取动作的多个可选部分的用户界面工具，所述多个可选部分至少包括：

用于阻塞来自所述第三方内容源的内容的可选按钮；以及

用于允许来自所述第三方内容源的内容的可选按钮。

14. 如权利要求 0 所述的计算机实现的方法，其特征在于，所述应用程序是 Web 浏览器。

15. 如权利要求 0 所述的计算机实现的方法，其特征在于，所述查明包括将所计算的已经遭遇来自所述第三方内容源的内容的次数与指示感觉到的风险级别的一个或多个阈值进行比较。

16. 一种系统，包括：

一个或多个计算机可读存储介质；

包含在所述一个或多个计算机可读介质上的计算机可读指令，所述计算机可读指令在被执行时实现一 Web 浏览器，所述 Web 浏览器被配置成：

计算第三方内容源为由所述 Web 浏览器导航到的网页提供内容的次数；

基于所计算的次数确定所述第三方内容源何时处于可以观察用户的浏览习惯的位置；以及

输出通知来传达所述第三方内容源处于可以观察所述用户的浏览习惯的位置。

17. 如权利要求 16 所述的系统，其特征在于，所述 Web 浏览器被配置成将所述通知输出为弹出窗口。

18. 如权利要求 16 所述的系统，其特征在于，所述 Web 浏览器被配置成将所述通知输出为所述 Web 浏览器的菜单栏项。

19. 如权利要求 16 所述的系统，其特征在于，输出的所述通知包括使得用户能够允许、阻塞或忽略被确定为处于可以观察浏览习惯的位置的所述第三方内容源的多个可选部分。

20. 如权利要求 16 所述的系统，其特征在于，所述 Web 浏览器被配置成：

维护描述网页中与来自第三方内容源的多个内容项遭遇的数据库，其中所述数据库被配置成存储将所述内容项中的每一个的统一资源指示符 (URI) 与其中遭遇所述内容项的网页进行匹配的数据；以及

至少部分地基于内容项的 URI 的相似性来合并所述数据库中的所述内容项以得出所计算的所述第三方内容源为网页提供内容的次数。

网页私隐风险检测

[0001] 背景

[0002] 网页可以含有对用户可能有用的许多不同类型的内容。一个典型的网页可以由各种各样的本机内容（例如，直接来自网页的主提供者的内容）以及来自一个或多个第三方内容源的第三方内容组成。例如，新闻网页可以被配置成含有本机内容，诸如来自新闻提供者的新闻文章、链接和图片，以及第三方内容，诸如来自各个第三方内容源的广告、链接、插件（体育滚动条、天气跟踪器等）和类似内容。

[0003] 导航浏览器来查看新闻网页的用户意识到与新闻网页的交互。然而，用户可能没有意识到还与提供新闻网页的内容的第三方内容源发生的交互。此外，通过多个网页访问的第三方内容源可能处于可以观察用户的浏览习惯的位置。因此，第三方内容源可能造成对用户的私隐风险。但是，在没有与第三方内容源的交互的知识的情况下，用户不能够处在可以针对可能观察用户的浏览习惯的这些第三方内容源采取动作的位置。

[0004] 概述

[0005] 提供本概述是为了以简化的形式介绍将在以下详细描述中进一步描述的一些概念。本概述并不旨在标识出所要求保护的主题的关键特征或必要特征，也不旨在用于限定所要求保护的主题的范围。

[0006] 各实施例能够实现可能引起对用户的私隐风险的第三方内容源的检测。在至少某些实施例中，可以处理经由浏览器导航到的网页来标识为该网页提供内容的第三方内容源。可以存储将第三方内容源与其中遭遇该第三方内容的网页进行相关的数据。随后可以分析数据来确定特定第三方何时处于可以观察用户的浏览习惯的位置。在一个示例中，在与相同内容和 / 或第三方内容源有关的网页数量超过可配置的阈值时，确定为私隐风险。响应于确定了私隐风险，可以用各种各样的方式来输出通知以向用户通知潜在危险的内容。

[0007] 在至少某些其他实施例中，通知可以经由自动呈现给用户的用户界面工具来作出以向用户通知潜在危险的第三方内容源。在某些情形中，用户界面工具以这样一种形式存在 :在遭遇网页的危险第三方内容时自动呈现警告消息。此外，在某些情形中，用户界面工具可以结合一个或多个可选部分，可以选择这些可选部分来使得用户能够访问采取各种动作的功能，诸如阻塞或允许来自该第三方内容源的内容等。

[0008] 附图简述

[0009] 在全部附图中，使用相同的标号来指示相同的特征。

[0010] 图 1 示出根据一个或多个实施例的其中可以采用本发明的原理的操作环境。

[0011] 图 2 是描述根据一个或多个实施例的方法中的各步骤的流程图。

[0012] 图 3 是描述根据一个或多个实施例的方法中的各步骤的流程图。

[0013] 图 4 示出根据一个或多个实施例的 Web 浏览器用户界面。

[0014] 图 5 示出根据一个或多个实施例的 Web 浏览器用户界面。

[0015] 图 6 是根据一个或多个实施例的系统的框图。

[0016] 详细描述

[0017] 概览

[0018] 各实施例能够实现对可能引起对用户的私隐风险的第三方内容源的检测。在至少某些实施例中，可以处理经由浏览器导航到的网页来标识为该网页提供内容的第三方内容源。可以存储将第三方内容源与其中遭遇该第三方内容的网页进行相关的数据。随后可以分析数据来确定特定第三方何时处于可以观察用户的浏览习惯的位置。在一个示例中，在与相同内容和 / 或第三方内容源有关的网页数量超过可配置的阈值时，确定为私隐风险。响应于确定了私隐风险，可以用各种各样的方式来输出通知以向用户通知潜在危险的内容。

[0019] 在至少某些其他实施例中，通知可以经由自动呈现给用户的用户界面工具来作出以向用户通知潜在危险的第三方内容源。在某些情形中，用户界面工具以这样一种形式存在 :在遭遇网页的危险第三方内容时自动呈现警告消息。此外，在某些情形中，用户界面工具可以结合一个或多个可选部分，可以选择这些可选部分来使得用户能够访问采取各种动作的功能，诸如阻塞或允许来自该第三方内容源的内容等。

[0020] 在以下讨论中，题为“操作环境”的章节仅描述其中可采用各实施例的一个环境。之后，题为“私隐风险检测示例”的章节描述了其中可以标识网页中的第三方内容并可以确定私隐风险的各实施例。接着，题为“风险通知示例”的章节描述了其中可以输出通知以向用户通知可能对用户是危险的第三方内容的各实施例。最后，提供了题为“示例系统”的章节并且该章节描述可用于实现一个或多个实施例的示例系统。

[0021] 操作环境

[0022] 图 1 在 100 处概括地示出根据一个或多个实施例的操作环境。环境 100 包括计算设备 102，计算设备 102 具有一个或多个处理器 104、一个或多个计算机可读介质 106 和驻留在计算机可读介质上并可由处理器执行的一个或多个应用程序 108。应用程序 108 可包括任何合适类型的应用程序，如作为示例而非限制，读取器应用程序、电子邮件应用程序、即时消息收发应用程序、以及各种其他应用程序。

[0023] 计算设备 102 包括 Web 浏览器 110 形式的应用程序 108，该应用程序 108 提供可供计算设备 102 的用户使用来通过诸如因特网之类的网络 112 导航到可从其接收或向其发送内容的一个或多个网站 114 的功能。Web 浏览器 110 可用于提供各种各样的用户界面 116，用户可以通过该用户界面与可从一个或多个网站 114 获得的内容交互。

[0024] 网站 114 可以包括主内容源和第三方内容源。如此处所使用的，主内容源指的是来自用户已经肯定地和 / 或有意地导航到的网站 114 和 / 或有关域内部的内容的源。主内容源与用户已将浏览器定向到的统一资源指示符 (URI) 的域密切相关联，和 / 或可以具有与该域的提供者相同的提供者。如此处所使用的，第三方内容源是除了主内容源之外的内容源。换言之，第三方内容源是来自用户已将浏览器定向到的域之外的源，并且一般可以具有与该域的提供者不同的提供者。

[0025] 此外，Web 浏览器 110 可以包括或以其他方式利用如上文和下文中所描述地运作的私隐模块 118。私隐模块 118 表示当用户与一个或多个网站 114 交互时可被提供给用户的各种各样的私隐特征。例如，私隐模块 118 可以实现对提供从网站 114 获得的网页中的内容的第三方内容源的标识。私隐模块 118 还可以确定第三方内容源所造成的私隐风险。具体地，私隐模块 118 可以用于确定第三方内容源何时处于可以观察计算设备 102 的用户

的浏览习惯的位置。

[0026] 在一个实施例中，可以经由各种子模块来提供私隐模块 118 的功能。在图 1 的示例中，私隐模块 118 被示为包括日志模块 120 和检测器模块 122。日志模块 120 表示标识网页中的第三方内容的功能。日志模块 120 还可以维护数据库来将描述 Web 浏览器 110 与网站 114 以及相关联内容的交互的数据记录在日志中或以其他方式对其进行编译。经由日志模块 120 编译的各种数据可以在图 1 所示的数据存储 124 中维护。

[0027] 检测器模块 122 表示用于按各种方式处理由日志模块 120 编译的数据的功能。通过该处理，检测器模块 122 可以监视 Web 浏览器 110 与第三方内容源的交互并确定特定第三方内容源何时引起潜在的私隐风险。检测器模块 122 还可用于响应于该第三方内容是潜在危险的而导致通知的输出。

[0028] 计算机可读介质 106 可包括，作为示例而非限制，通常与计算设备相关联的所有形式的易失性和非易失性存储器和 / 或存储介质。这种介质可包括 ROM、RAM、闪存、硬盘、可移动介质等。计算设备的一个具体示例以下在图 6 中示出并描述。

[0029] 计算设备 102 可被具体化为任何合适的计算设备，诸如作为示例而非限制，台式计算机，便携式计算机，诸如个人数字助理 (PDA)、蜂窝电话等手持式计算机，等等。

[0030] 考虑了示例操作环境之后，现在考虑其中可以检测与来自第三方内容源的内容相关联的私隐风险的各实施例的讨论。

[0031] 私隐风险检测示例

[0032] 在一个或多个实施例中，可以采用各种技术来标识与出现在网页上的内容相关联的第三方内容源。如上所述，可以编译并存储各种数据来将第三方内容源与其中遭遇来自该第三方内容源的内容的网页进行相关。可以处理将第三方内容源与网页进行相关的数据来检测可能引起私隐风险的那些第三方内容源。

[0033] 图 2 是描述根据一个或多个实施例的方法中的各步骤的流程图。该方法可以结合任何合适的硬件、软件、固件或其组合来执行。在至少某些实施例中，该方法可以由诸如以上在图 1 描述的 Web 浏览器 110 等经合适配置的 Web 浏览器执行。

[0034] 步骤 200 接收与网页相关联的 HTML 代码。该步骤可以在 Web 浏览器导航到特定网页时执行。步骤 202 处理 HTML 代码并且步骤 204 标识该网页中来自第三方内容源的内容。该步骤可以用任何合适的方式来执行。例如，与该网页相关联的 HTML 代码可以标识要被包括在用户可以订阅的网页中的内容。可以如何完成该步骤的一个示例是通过 HTML 标签、URI 以及嵌入在 HTML 代码中的其他合适的标识符。只要对 HTML 代码的处理导致下载要包括在网页中的内容的请求时便可出现标识。

[0035] 如上所述，可以从主内容源和第三方内容源两者提供网页中的内容。因此，步骤 204 中的标识可以包括在主内容源和第三方内容源之间进行区分。在一个或多个实施例中，可以在所请求内容的路径和该内容出现在其中的网页的路径之间作出比较来确定所请求内容的源是否在与 Web 浏览器被定向到的网页相同的域中和 / 或是否具有与 Web 浏览器被定向到的网页相同的提供者。当域和 / 或提供者被确定为不同时，可以将所请求内容标识为来自第三方内容源的内容。

[0036] 响应于标识一个或多个第三方内容源，步骤 206 存储将该一个或多个第三方内容源与网站进行相关的数据。之后，步骤 208 监视与该一个或多个第三方内容源的交互来确

定潜在的私隐风险。

[0037] 例如，基于对来自第三方源的内容的标识，可以编译数据并将该数据存储在数据库中，诸如图 1 的数据存储 124 内的日志中。在第一次标识第三方内容源时，可以将该第三方内容源的记录添加到数据库。该记录将该第三方内容源与其中遭遇来自该第三方内容源的内容的网站进行相关。之后，每一次 Web 浏览器遭遇该第三方内容源时便更新数据库中的记录来反映浏览器被导航到的可能的其他网页中的附加遭遇。

[0038] 在一个或多个实施例中，数据库中维护的记录用于将不同的网站 / 域已经遭遇了第三方内容源多少次记录在日志中或以其他方式对其进行跟踪。例如，特定第三方内容源的记录可以包括每一次不同的网站和 / 或域遭遇该特定第三方内容源时可以递增的计数字段。遭遇第三方内容源的次数可以是用于确定该第三方内容源对用户造成多少私隐风险的基础。

[0039] 考虑经由 Web 浏览器 110 在网页输出中遭遇的一个特定第三方内容源。当遭遇该第三方内容源时，Web 浏览器 110 诸如通过私隐模块 118 可以引用数据存储 124 来确定是否存在关于该第三方内容源的记录。假定记录已经存在，则 Web 浏览器 110 还可用于确定该第三方内容源是否已经与该网页相关。假定该第三方内容源尚未与该网页相关，则 Web 浏览器 110 可以更新记录来反映该附加遭遇并且还可以递增与该记录相关联的计数器来指示不同的网站和 / 或域已经遭遇该第三方内容源的次数。

[0040] 在一个或多个实施例中，Web 浏览器至少部分地基于已经遭遇第三方内容源的次数来确定该第三方内容源所造成的风险。如上所述地递增计数器是 Web 浏览器可以怎样达到次数的一个示例。例如，如果在站点 A 和站点 B 两处都遭遇内容项“source1.xyz.foo.js”，则“source1.xyz.foo.js”的源可以具有足够的信息来知晓该 Web 浏览器已经访问过站点 A 和 B。还可以通过与第三方源的交互来交换诸如 IP 地址、浏览器设置、偏好等其他信息。在该示例中，将计数器值设为“2”，该计数器值对应于遭遇“source1.xyz.foo.js”的不同站点的数量。

[0041] 在一个或多个实施例中，Web 浏览器可以实现可以用来将计数器值（例如，不同站点的数量）与一个或多个感觉到的风险级别进行相关的可配置阈值。可以采用与不同风险级别相关联的单个阈值或多个值范围。作为示例而非限制，下表 1 提供了可以用来确定感觉到的风险级别的、与不同的风险级别相关联的多个值范围的一个示例。

[0042] 表 1 :感觉到的风险级别对第三方遭遇

[0043]

[0044]

风险级别	遭遇次数
低	0-5
中	6-10
高	11 或更多

[0045] 因此，按照上文和下文中所描述的方式，诸如图 1 所述的 Web 浏览器 110 之类的经合适配置的 Web 浏览器可以监视与第三方内容源的交互并确定与该第三方内容源相关联

的私隐风险。图 3 的以下讨论提供了可以采用来确定与第三方内容源相关联的私隐风险的各技术的附加示例。

[0046] 图 3 是描述根据一个或多个实施例的方法中的各步骤的流程图。该方法可以结合任何合适的硬件、软件、固件或其组合来执行。在至少某些实施例中，该方法可以由诸如以上在图 1 描述的 Web 浏览器 110 等经合适配置的 Web 浏览器执行。

[0047] 步骤 300 标识在网页中遭遇的第三方内容源。该步骤可以用任何合适的方式来执行。在 Web 浏览器处理特定网页的 HTML 代码并生成从一个或多个内容源下载内容时可以执行该步骤。例如，与网页相关联的 HTML 代码可以标识要被包括在该网页中的内容。可以如何完成该步骤的一个示例是通过 HTML 标签、URI 以及嵌入在 HTML 代码中的其他合适的标识符。在至少某些实施例中，对第三方内容的标识可以替换地在已经呈现了网页之后出现。可以采用这种技术来避免在呈现网页期间消费处理资源和相应的性能损失。

[0048] 步骤 302 更新被维护来将网页与第三方内容源进行相关的数据库。具体地，Web 浏览器诸如通过图 1 的日志模块 120 可以更新数据库中对应于该第三方内容源的记录来反映该网页已经遭遇过该第三方内容源。如果对应于该第三方内容源的记录尚未存在，则可以创建新的记录。

[0049] 之后，步骤 304 分析数据库来确定该第三方内容源引起的私隐风险。具体地，Web 浏览器诸如通过图 1 的检测器模块 122 可以按各种方式来分析数据库中的数据以确定第三方内容源是否处于可以观察用户的浏览习惯的位置。

[0050] 在一个或多个实施例中，分析数据库可以包括合并数据库中的相似项。可以应用各种逻辑来合并相似项。合并项可以在不同内容项的路径数据的基础上来执行。作为示例而非限制，路径数据可以包括 URI、文件名、查询串、参数、主域名及其组合。可以作出两个内容项的路径数据的比较。当内容项足够相似时，该内容项的数据可以被分组在一起来确定是否存在造成私隐风险的第三方内容源。

[0051] 例如，考虑具有路径 http://www.tracku.com/1234/foo.js 的一个第三方内容项和具有路径 http://www.tracku.com/5678/foo.js 的第二个第三方内容项。在该示例中，域“www.tracku.com”和文件名“foo.js”是相同的。基于这些相似性，被应用来分析数据库的逻辑可以导致对应于该两项的数据被合并。具体地，该两个内容项可以都与同一个第三方内容源，例如“www.tracku.com”相关联。构想了用于合并相似项的各种不同的技术和算法。

[0052] 在一个或多个实施例中，分析数据库还可以包括确定已经遭遇第三方内容源和 / 或项的次数。确定次数的一个示例是经由每一次不同的网站和 / 或域遭遇第三方内容源时递增计数字段，如先前所描述的。一般而言，计数越高，潜在的私隐风险越大。构想了适于得出已经遭遇第三方内容源和 / 或项的次数的各种算法。作为示例而非限制，如下在表 2 中提供了可以采用的一个示例风险检测算法：

[0053] 表 2 :示例风险检测算法

[0054] 给定数据库 d，主网站 f 和被标识为将内容提供给主网站 f 的第三方内容源 t，可以在 d 中存储将 f 和 d 作为对 (f，t) 进行相关的数据：

[0055] 当 tracker.FQDN 等于 t.FQDN 时从 d 中选择所有第三方

[0056] 如果第三方为空，则将 t 作为新的项添加到 d，且计数为 1。

[0057] 否则

[0058] 对于第三方中的每一个第三方 T

[0059] 如果 T 匹配正则表达式“t.FQDNV.*Vt.filename”

[0060] 将布尔匹配设为等于假

[0061] 对于 T.PrimaryWebSites 中的每一个主网站 F

[0062] 如果 f 等于 F

[0063] 将匹配设为等于真

[0064] 如果匹配等于假

[0065] 将 f 添加到 T.PrimaryWebSites

[0066] 递增 T.Primary WebSites

[0067] 否则，丢弃 (f，t) 并退出

[0068] 否则，丢弃 (f，t) 并退出

[0069] 基于数据库的分析，步骤 306 确定第三方内容源是否引起私隐风险。可以如何完成该步骤的一个示例是通过如先前所讨论的一个或多个阈值。当在步骤 306 中未确定足够的私隐风险的情况下，步骤 308 继续监视网页和 / 或第三方源来检测私隐风险。例如，在经由 Web 浏览器呈现附加网页时，可以采用上文和下文中所描述的各种技术来检测来自这些网页中遭遇的第三方内容源的私隐风险。

[0070] 当在步骤 306 中确定足够的私隐风险的情况下，步骤 310 输出私隐风险的通知以通知用户。可以使用任何合适的通知来向用户通知第三方内容源所引起的风险。在一个或多个实施例中，通知可以经由自动呈现给用户的用户界面工具来作出以向用户通知被确定为潜在危险的第三方内容源。在至少某些实施例中，该用户界面工具可以用响应于检测到潜在危险的第三方内容源而自动输出的弹出窗口或对话框的形式输出。在其他实施例中，通知可以用可以出现在 Web 浏览器的菜单栏中的菜单栏项的形式输出。可以在下文中题为“风险通知示例”的章节中找到可以输出的某些合适的示例通知的其他讨论。

[0071] 在一个或多个实施例中，输出通知的用户界面工具可以包括使得用户能够针对第三方内容源采取动作的一个或多个可选部分。例如，弹出窗口或对话框形式的通知可以包括可由用户选择来使得用户能够访问用作阻塞和 / 或允许来自该第三方内容源的内容的功能的一个或多个可选按钮或其他合适的控件。因此，通过与用户界面工具的交互，用户可以提供输入来发起针对潜在危险的第三方内容源的各种动作。

[0072] 步骤 312 确定可以响应于潜在危险的第三方内容源的通知来接收的用户输入。当接收到允许第三方内容源的用户输入时，步骤 314 允许该第三方内容源内容。同样，当接收到阻塞第三方内容源的用户输入时，步骤 316 阻塞来自该第三方内容源的内容。

[0073] 允许和阻塞内容的一种方式可以通过描述了 Web 浏览器要允许和阻塞的内容源的一个或多个控制列表来发生。可以基于接收到指示要阻塞还是允许特定第三方内容源的用户输入来更新控制列表。在一个或多个实施例中，用户可以根据用户的浏览习惯来填充控制列表。因此，可以避免如某些传统的系统中采用的创建和维护预先填充的控制列表的时间和费用。根据上述实施例的控制列表可以在诸如图 1 所描绘的数据存储 124 之类的数据库中维护。在呈现内容时，Web 浏览器可以引用和利用控制列表并根据控制列表中指定的被允许和 / 或阻塞的内容来动作。

[0074] 虽然在上述示例中已经描述了允许或阻塞内容的用户输入，但构想了可以针对被检测为潜在危险的第三方内容源采用的各种其他用户输入和相应的动作。作为示例而非限制，可以通过合适的用户输入来发起的其他示例动作可以包括：获得关于第三内容的更多信息、设置关于该内容的提醒、访问社交网络来寻求推荐、和/或忽略通知（例如，不采取进一步的动作）。

[0075] 在描述了其中可以发生检测潜在危险的第三方内容的示例实施例之后，现在考虑其中可以将潜在危险的第三方内容源的通知输出给用户的其他实施例。具体地，在以下描述的各实施例中，描述了出于可以响应于检测到潜在危险的第三方内容源而输出的风险通知的读者的利益而提供有形示例的示例用户界面。

[0076] 风险通知示例

[0077] 如先前所讨论的，Web 浏览器可以实现上文和下文中所描述的各种技术来检测可能处于可以观察浏览习惯的位置的第三方内容源，例如潜在危险的第三方内容源。响应于这种检测，可以输出通知来向用户通知该潜在危险的第三方内容源，并使得用户能够针对该第三方内容源采取动作。

[0078] 图 4 在 400 处概括地示出其中网页 402 被描绘为正被呈现的 Web 浏览器用户界面。所示用户界面只是可被输出来实现与可从一个或多个网站 114 获得的内容的各种用户交互的图 1 的用户界面 116 的一个示例。如先前所讨论的，所呈现的网页 402 可以包括来自各种源的内容，包括主内容源和一个或多个第三方内容源。在所示示例中，“最新新闻”部分 404 和各链接 406 表示来自诸如 Web 浏览器已经被定向到的网页 402 的提供者之类的主内容源的内容。汽车图像 408、高尔夫相关广告 410 和天气插件 412 表示网页 402 中已从一个或多个第三方内容源获得的内容。

[0079] 为了呈现网页 402，Web 浏览器可以处理与网页 402 相关联的 HTML 代码。根据上文和下文中所描述的各种技术，经合适配置的 Web 浏览器可用于检测潜在危险的第三方内容源。这种检测可以至少部分地通过处理相关联网页的 HTML 代码来发生。响应于检测到潜在危险的内容，可以输出通知来通知用户并允许针对潜在危险的内容的各种动作。

[0080] 参考图 5，再次描绘了图 4 的用户界面 400 和网页 402。在该示例中，Web 浏览器已经检测到网页 402 中可能引起私隐风险的内容。因此，已经输出通知来向用户通知潜在的风险。

[0081] 在这种情况下，输出通知被示为经由可以经由 Web 浏览器显示的用户界面工具来提供。可以使用任何合适的用户界面工具来提供这种通知。在所示示例中，用户界面工具用弹出窗口 502 的形式来显示私隐通知。更具体地，私隐通知指示“bannerad.ps”内容项已经被检测为是潜在危险的。该示例中的“bannerad.ps”项对应于高尔夫相关广告 410，该广告已经从例如“adserver.com”等第三方内容源获得。通知的输出响应于确定在用户访问的多个不同的网站处遭遇了“adserver.com”而发生。例如，示例私隐通知指示已经存在“6”次遭遇并指派风险级别“中”。确定遭遇的次数和风险级别的指派可以根据此处描述的计数和各种可配置阈值来发生。

[0082] 弹出窗口 502 被示为包括使得用户能够针对第三方内容源采取动作的可选部分的各种示例。具体地，示例弹出窗口 502 包括允许按钮 504、阻塞按钮 506、忽略按钮 508 和更多信息链接 510。

[0083] 通过在允许按钮 504 上点击，用户可以提供输入来使得“bannerad.ps”项和 / 或“adserver.com”被标识为被允许内容。可以出现这种情况的一种方式是通过将这些项添加到被允许内容控制列表。同样，通过在阻塞按钮 506 上点击，用户可以提供输入来使得“bannerad.ps”项和 / 或“adserver.com”被标识为被阻塞内容。再一次，这种情况可以通过将这些项添加到被阻塞内容控制列表来发生。通过在忽略按钮 508 上点击，用户可以提供输入来忽略该输出通知。在这种情况下，用户可以推迟对该内容的决定直到再次遭遇该内容的另一时刻。

[0084] 更多信息链接 510 可以提供一种机制，用户可以通过该机制来获得向用户通知关于所检测的第三方内容源的更多信息，从而帮助用户决定是允许还是阻塞该第三方内容源。通过选择更多信息链接 510，可以将 Web 浏览器重定向到关于潜在危险的第三方内容源的信息的各种源。作为示例，用户对更多信息链接 510 的选择可以将 Web 浏览器重定向到收集并提供关于各种第三方内容源的信息的服务。在另一示例中，用户对更多信息链接 510 的选择可以将 Web 浏览器重定向到编译来自用户的社区的关于第三方内容源的推荐的社交团体站点。

[0085] 在又一示例中，用户对更多信息链接 510 的选择可以将 Web 浏览器重定向到该第三方内容源所提供的网页。在该示例中，第三方内容源可以提供该第三方内容源可以通过其来提供关于它们在网页中提供的内容的附加信息的功能。可以出现这种情况的一种方式是通过用特定标志、HTML 标签或指示该附加信息可用的其他合适的数据来配置与来自第三方内容源的内容相关联的 HTML 代码。还可以将使得 Web 浏览器重定向到附加信息的路径名嵌入到该内容的 HTML 代码中。Web 浏览器可以识别特定标志、HTML 标签或指示该附加信息可用的其他合适的数据。Web 浏览器随后可以构造更多信息链接 510 来将 Web 浏览器重定向到该第三方内容源指定的路径名。以此方式，第三方内容源能够帮助用户更好地理解该第三方内容源所提供的内容、该第三方内容源所收集的信息、如何使用该第三方内容源所收集的信息等等。至少部分地基于该信息，用户可以关于是阻塞还是允许被检测为潜在危险的内容或内容源作出有见识的决定。

[0086] 图 5 还将菜单栏项 512 描绘为适于提供风险通知的用户界面工具的另一替换示例。菜单栏项 512 可以响应于检测到潜在危险的一个或多个第三方内容源而自动地出现在 Web 浏览器的菜单栏中。菜单栏项 512 可以在除了或代替诸如弹出窗口 502 等其他用户界面工具的情况下出现。菜单栏项 512 可以包括用户可以与其交互来获得关于所检测的风险的信息的下拉框特征。例如，用户与菜单栏项 512 的交互可以导致在下拉框中与如在弹出窗口 502 中呈现的所示信息和控件相似的私隐通知的显示。

[0087] 虽然已经讨论了弹出窗口 502 和菜单栏项 512 的示例，但还可以构想可以通过其来作出风险通知的各种其他用户界面工具。作为示例而非限制，风险通知可以经由 Web 浏览器面板、Web 浏览器信息窗格、出现在工具栏或边栏中的操作系统消息、和 / 或适于呈现与网页中遭遇的内容有关的风险通知的任何其他用户界面工具来作出。通知还可以通过其他类型的通信来作出，诸如通过即时消息或电子邮件。在一个或多个实施例中，用户可以响应于检测到潜在危险的第三方内容源来选择要接收的一个或多个所需类型的通知。

[0088] 在描述了其中采用了各种技术来检测可能造成私隐风险的第三方内容源的各实施例之后，现在考虑可被用来实现以上所述的各实施例的示例系统的讨论。

[0089] 示例系统

[0090] 图 6 示出可以实现上述各实施例的示例计算设备 600。计算设备 600 可以是例如图 1 的计算设备 102 或任何其他合适的计算设备。

[0091] 计算设备 600 包括一个或多个处理器或者处理单元 602、一个或多个存储器和 / 或存储组件 604、一个或多个输入 / 输出 (I/O) 设备 606、以及允许各组件和设备彼此通信的总线 608。总线 608 表示任何若干类型的总线结构中的一个或多个，包括存储器总线或存储器控制器、外围总线、加速图形端口、以及使用各种总线体系结构的任一种的处理器或局部总线。总线 608 可包括有线和 / 或无线总线。

[0092] 存储器 / 存储组件 604 表示一个或多个计算机存储介质。组件 604 可包括易失性介质（如随机存取存储器 (RAM)）和 / 或非易失性介质（如只读存储器 (ROM)、闪存、光盘、磁盘等等）。组件 604 可包括固定介质（例如，RAM、ROM、固定硬盘驱动器等）以及可移动介质（例如闪存驱动器、可移动硬盘驱动器、光盘等等）。

[0093] 一个或多个输入 / 输出设备 606 允许用户向计算设备 600 输入命令和信息，并且还允许向用户和 / 或其他组件或设备呈现信息。输入设备的示例包括键盘、光标控制设备（例如鼠标）、话筒、扫描仪等。输出设备的示例包括显示设备（例如监视器或投影仪）、扬声器、打印机、网卡等。

[0094] 各种技术在此可以在软件或程序模块的一般上下文中描述。一般而言，软件包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。这些模块和技术的实现可以存储在某种形式的计算机可读介质上或通过某种形式的计算机可读介质传输。计算机可读介质可以是可由计算机访问的任何一个或多个可用介质。作为示例而非限制，计算机可读介质可以包括“计算机存储介质”。

[0095] “计算机存储介质”包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括但不限于，RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘 (DVD) 或其他光盘存储、盒式磁带、磁带、磁盘存储或其他磁存储设备，或者可用于存储所需信息并可由计算机访问的任何其他介质。

[0096] 结论

[0097] 本文描述了能够实现对网页中可能引起私隐风险的第三方内容源的检测的各实施例。

[0098] 尽管已经用结构特征和 / 或方法步骤专用的语言描述了本主题，但要理解，所附权利要求书中定义的主题不必限于所描述的具体特征或步骤。相反，这些具体特征和步骤是作为实现所要求保护的主题的示例性形式而公开的。

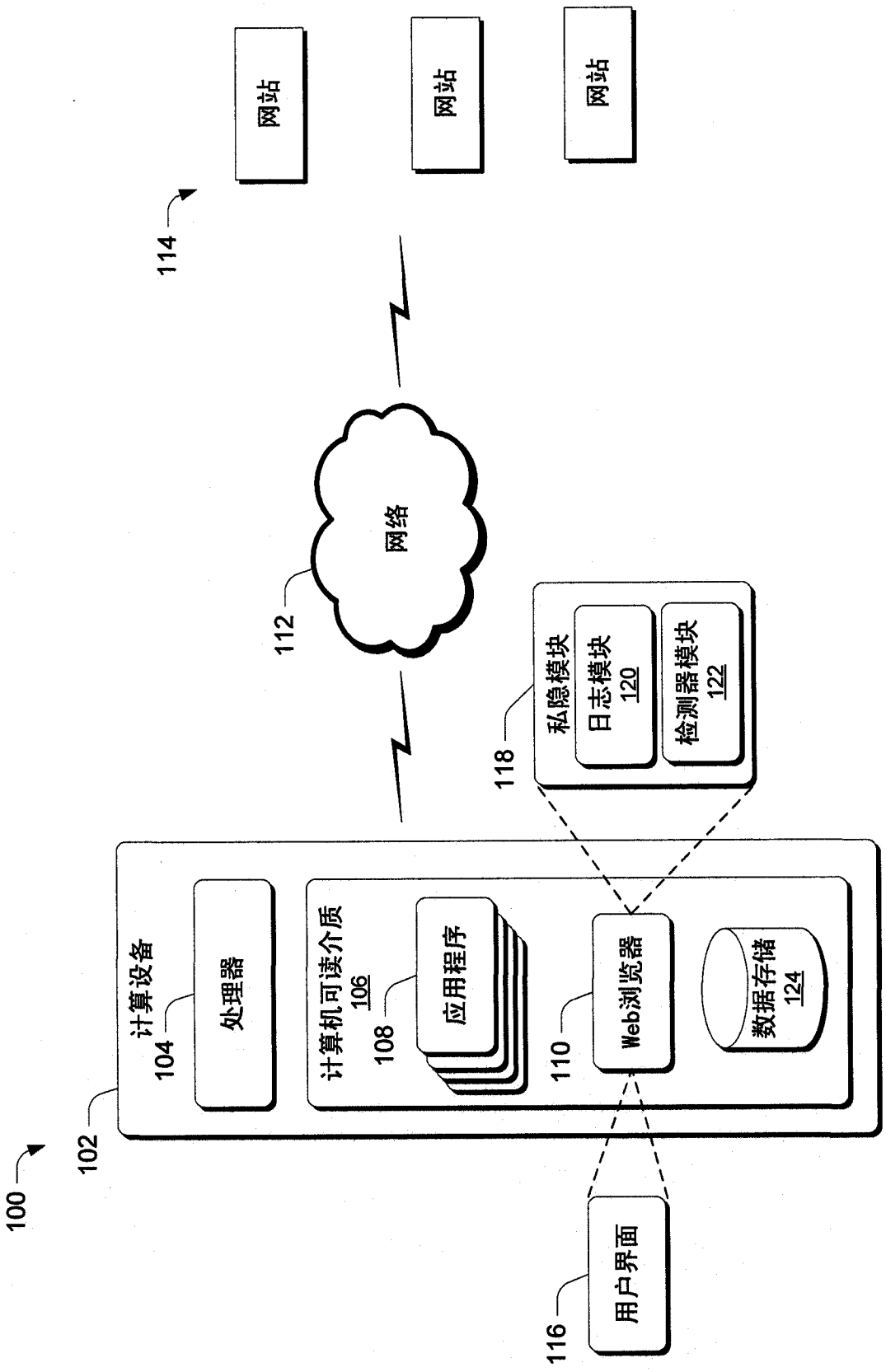

网站
网站
网站
114
网络
112
私隐模块
日志模块
120
检测器模块
122
118
计算设备
104
处理器
计算机可读介质
106
108
应用程序
110
Web浏览器
数据存储
124
102
100
用户界面
116

图 1

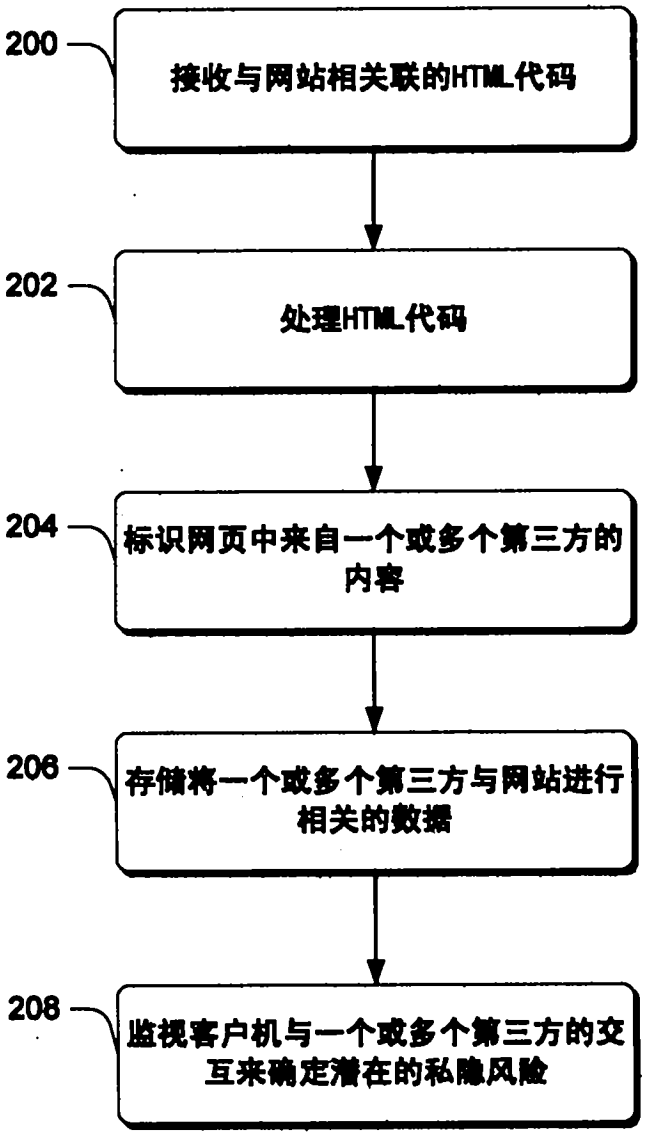

200
接收与网站相关联的HTML代码
202
处理HTML代码
204
标识网页中来自一个或多个第三方的内容
206
存储将一个或多个第三方与网站进行相关的数据
208
监视客户机与一个或多个第三方的交互来确定潜在的私隐风险

图 2

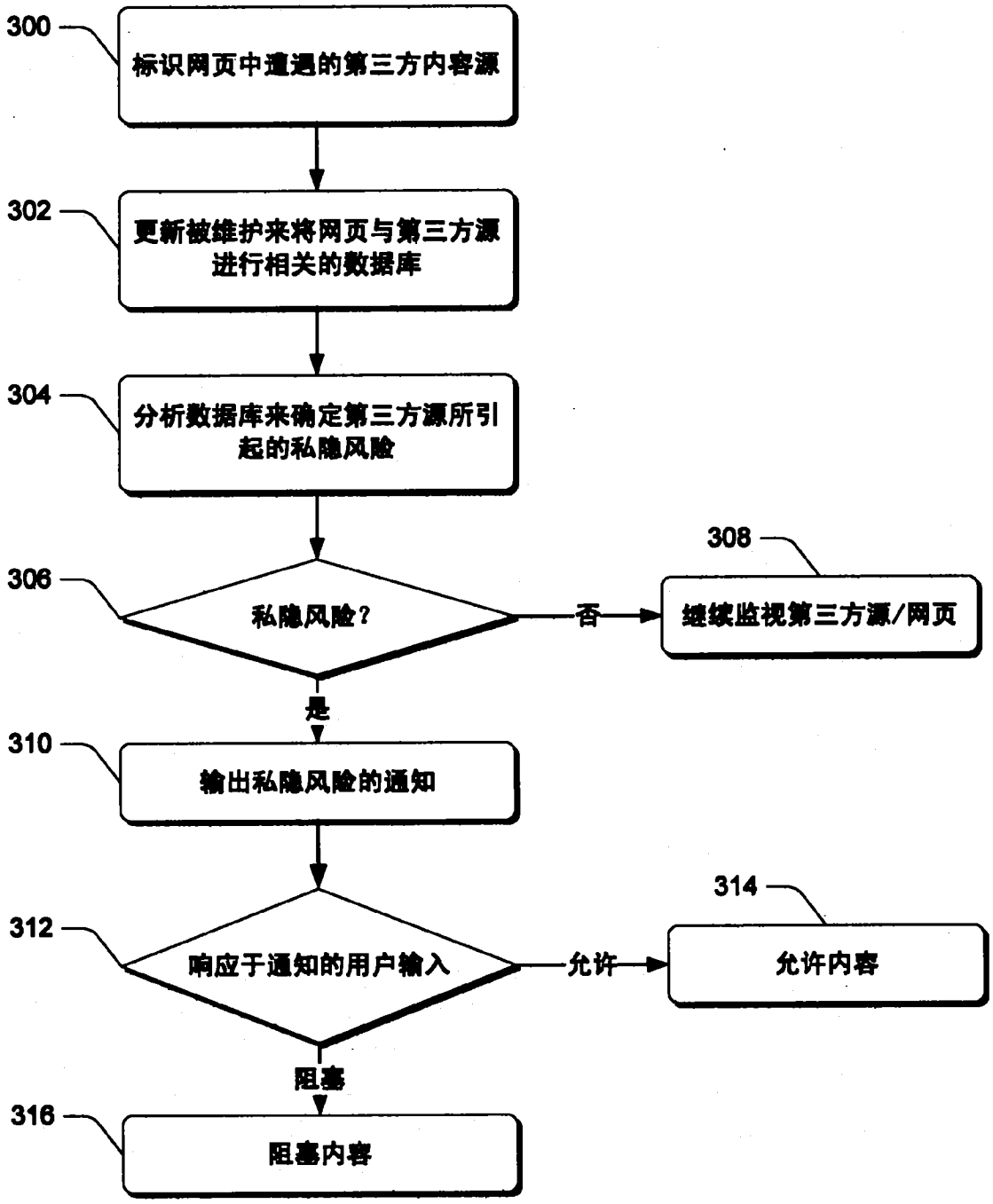

300
标识网页中遭遇的第三方内容源
302
更新被维护来将网页与第三方源进行相关的数据库
304
分析数据库来确定第三方源所引起的私隐风险
306
私隐风险？
否
308
继续监视第三方源/网页
是
310
输出私隐风险的通知
312
响应于通知的用户输入
允许
314
允许内容
阻塞
316
阻塞内容

图 3

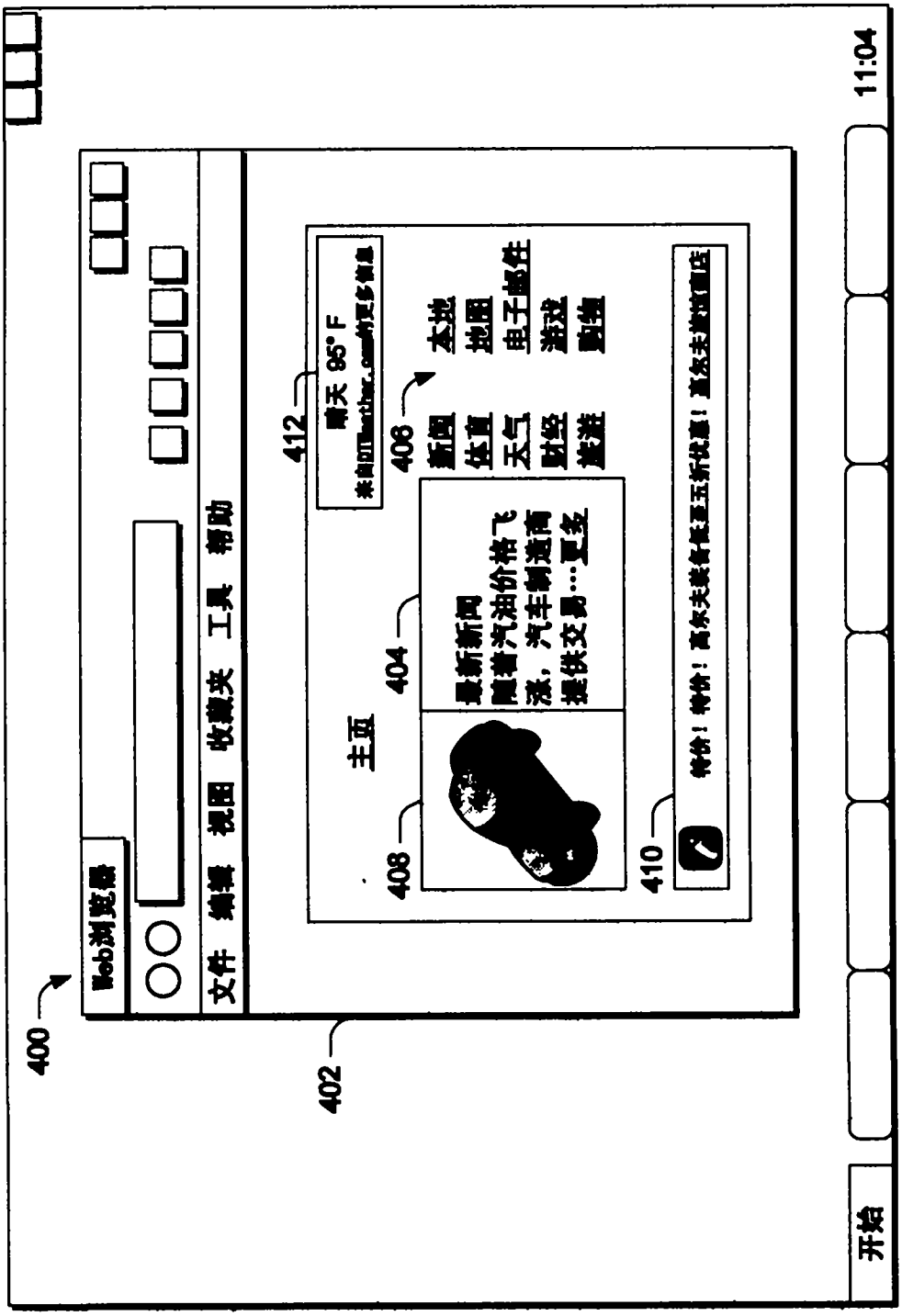

11:04
开始
Web浏览器
文件 编辑 视图 收藏夹 工具 帮助
400
402
主页
404
408
412
410
新闻 本地
体育 地图
天气 电子邮件
财经 游戏
旅游 购物

图 4

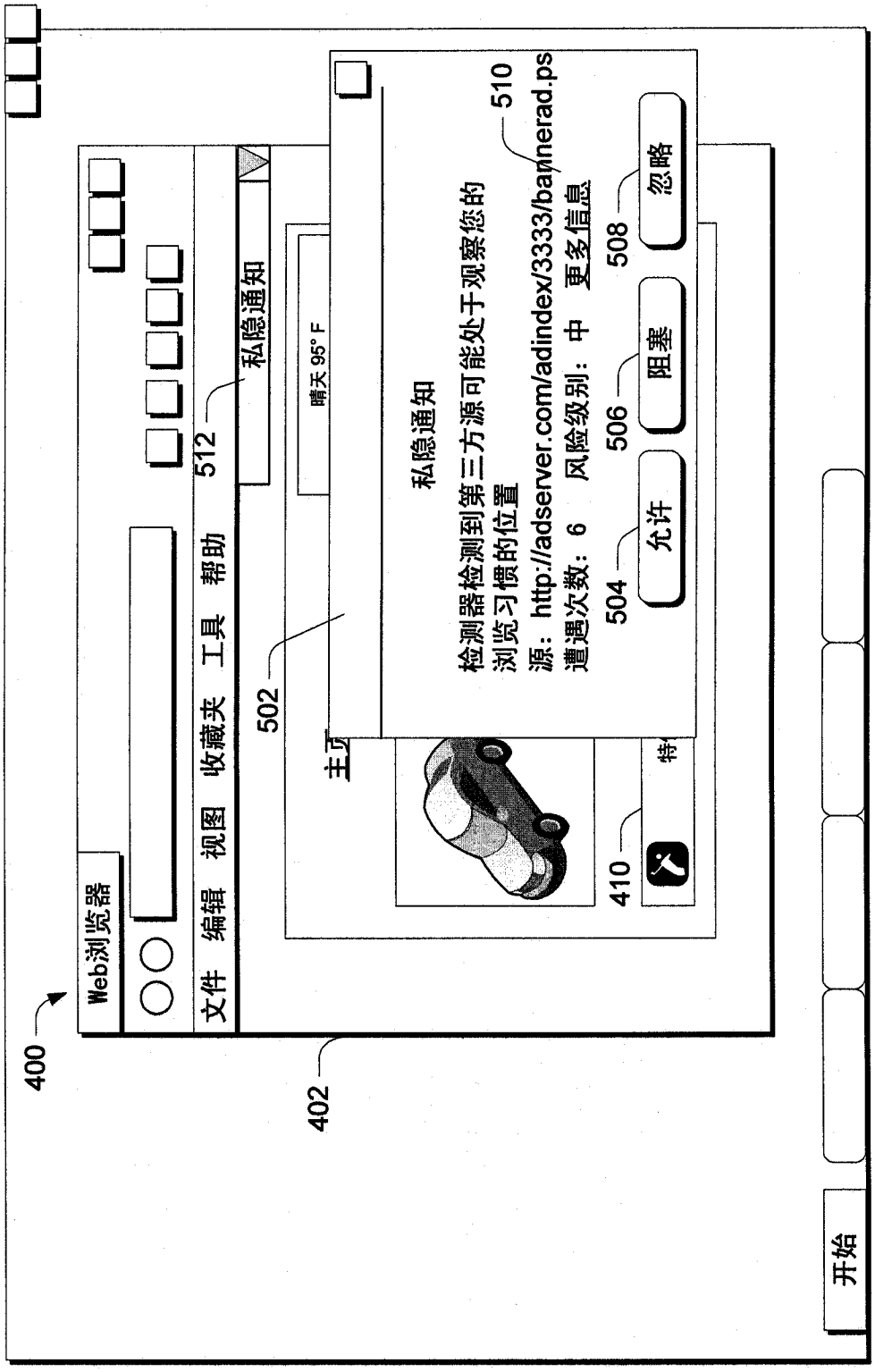

400
Web浏览器
文件 编辑 视图 收藏夹 工具 帮助
512
私隐通知
晴天 95° F
502
402
私隐通知
检测器检测到第三方源可能处于观察您的浏览习惯的位置
510
源：http://adserver.com/adindex/3333/banner.ps
遭遇次数：6 风险级别：中 更多信息
504
允许
506
阻塞
508
忽略
410
开始

图 5

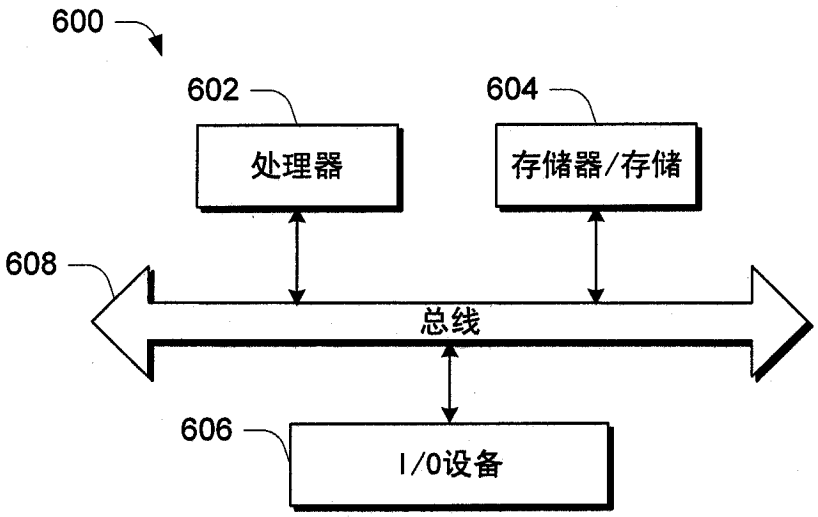


图 6