(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 113688033 A
(43)申请公布日 2021.11.23

(21)申请号 202110817930.6

(22)申请日 2021.07.20

(71)申请人 荣耀终端有限公司
地址 518040 广东省深圳市福田区香蜜湖街道东海社区红荔西路8089号深业中城6号楼A单元3401

(72)发明人 郝占峰

(74)专利代理机构 上海音科专利商标代理有限公司 31267
代理人 贾玉

(51)Int.Cl.
G06F 11/36(2006.01)

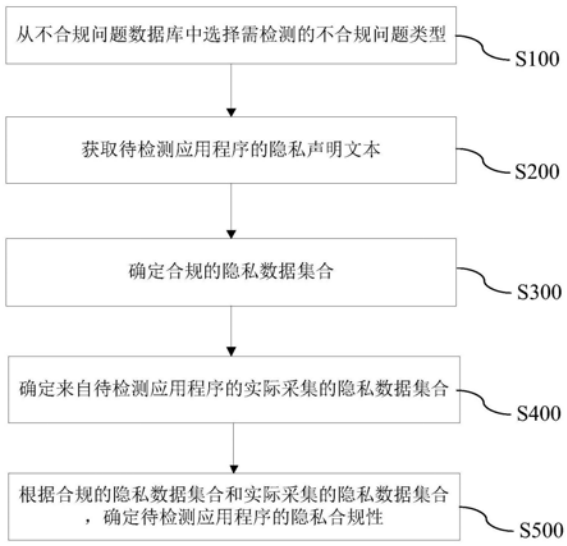
权利要求书2页 说明书15页 附图7页

(54)发明名称

一种隐私合规检测方法及计算机可读存储介质

(57)摘要

本申请涉及电子设备领域，公开了一种隐私合规检测方法及计算机可读存储介质。检测方法包括：从不合规问题数据库中选择需检测的不合规问题类型，不合规问题数据库中存储多个不合规问题类型；获取待检测应用程序的隐私声明文本；根据选择的需检测的不合规问题类型和待检测应用程序，确定合规的隐私数据集合；根据隐私声明文本和/或待检测应用程序的源码，确定来自待检测应用程序的实际采集的隐私数据集合；根据合规的隐私数据集合和实际采集的隐私数据集合，确定待检测应用程序的隐私合规性。可针对不同的不合规问题类型创建检测分析模型，保证应用程序的隐私合规检测的针对性更强。



CN 113688033 A

1.一种应用程序的隐私合规检测方法,其特征在于,所述方法包括:

从不合规问题数据库中选择需检测的不合规问题类型,所述不合规问题数据库中存储多个不合规问题类型;

获取待检测应用程序的隐私声明文本;

根据选择的所述需检测的不合规问题类型和所述待检测应用程序,确定合规的隐私数据集合;

根据所述隐私声明文本和/或所述待检测应用程序的源码,确定来自所述待检测应用程序的实际采集的隐私数据集合;

根据所述合规的隐私数据集合和所述实际采集的隐私数据集合,确定所述待检测应用程序的隐私合规性。

2.如权利要求1所述的检测方法,其特征在于,所述不合规问题类型包括:过度收集问题,所述过度收集问题是指所述实际采集的隐私数据集合超过了所述合规的隐私数据集合。

3.如权利要求2所述的检测方法,其特征在于,所述合规的隐私数据集合包括个人隐私数据集合,所述实际采集的隐私数据集合包括个人隐私数据集合和非个人隐私数据集合。

4.如权利要求1所述的检测方法,其特征在于,所述不合规问题类型包括:持续收集问题,所述持续收集问题是指所述隐私声明文本描述的内容和所述待检测应用程序所发布的国家或地区的标准文件不对应,所述标准文件由隐私合规监管机构颁布。

5.如权利要求1至4任一项所述的检测方法,其特征在于,所述确定合规的隐私数据集合,包括:从预先采集的合规的隐私数据集合库中确定相对应的合规的隐私数据集合。

6.如权利要求1至4任一项所述的检测方法,其特征在于,所述确定合规的隐私数据集合,包括:通过扫描所述隐私声明文本确定合规的隐私数据集合。

7.如权利要求6所述的检测方法,其特征在于,所述通过扫描所述隐私声明文本确定合规的隐私数据集合,包括:通过扫描所述隐私声明文本声明的实现设定功能需采集的隐私数据集合确定为所述合规的隐私数据集合。

8.如权利要求1至4任一项所述的检测方法,其特征在于,所述确定合规的隐私数据集合,包括:

获取所述需检测的不合规问题类型和所述待检测应用程序对应的标准文件,所述标准文件由隐私合规监管机构颁布;

从所述标准文件中确定合规的隐私数据集合。

9.如权利要求1至8任一项所述的检测方法,其特征在于,所述确定来自所述待检测应用程序的实际采集的隐私数据集合,包括:

扫描所述隐私声明文本;

从所述隐私声明文本中获取所述待检测应用程序的功能和隐私数据的关联关系,确定所述待检测应用程序的功能和隐私数据的关联关系为所述实际采集的隐私数据集合。

10.如权利要求1至8任一项所述的检测方法,其特征在于,所述确定来自所述待检测应用程序的实际采集的隐私数据集合,包括:

扫描所述待检测应用程序的源码;

对所述源码进行解析,获取所述待检测应用程序的功能和隐私数据的关联关系,确定

所述待检测应用程序的功能和隐私数据的关联关系为所述实际采集的隐私数据集合。

11.如权利要求10所述的检测方法，其特征在于，所述获取所述待检测应用程序的功能和隐私数据的关联关系，包括：

对所述源码进行解析，获取所述待检测应用程序的功能、代码类和方法的对应关系；

遍历所述待检测应用程序的功能，获取所述代码类和隐私数据的对应关系；

根据所述待检测应用程序的功能、代码类和方法的对应关系，以及所述代码类和隐私数据的对应关系获取所述待检测应用程序的功能和隐私数据的关联关系。

12.如权利要求1所述的检测方法，其特征在于，所述确定来自所述待检测应用程序的实际采集的隐私数据集合，包括：

根据所述隐私声明文本，检测系统反馈信息和/或用户输入的信息；

根据所述系统反馈信息和/或所述用户输入的信息，确定来自所述待检测应用程序的实际采集的隐私数据集合。

13.如权利要求12所述的检测方法，其特征在于，所述方法还包括：检测所述待检测应用程序的网络请求，根据所检测的网络请求结果、所述合规的隐私数据集合和所述实际采集的隐私数据集合，确定所述待检测应用程序的隐私合规性。

14.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有指令，该指令在计算机上执行时使得计算机执行权利要求1至13任一项所述的检测方法。

一种隐私合规检测方法及计算机可读存储介质

技术领域

[0001] 本申请涉及电子设备领域,特别涉及一种隐私合规检测方法及计算机可读存储介质。

背景技术

[0002] 当前用户的隐私保护意识越来越强,世界国家对隐私保护也变得越来越重视,并且对隐私保护的要求也各不相同。随着科技的发展,手机APP(application software,应用软件)也快速发展,为了满足用户不同的需求,手机中所安装的APP也越来越多。用户在使用手机APP的过程中,App会收集个人数据。但,APP在收集个人数据过程中会出现很多不合规的收集场景,这些场景可能会引起隐私安全。对于不合规手机个人数据的APP,相关管理机构会通知APP运营方进行整改,对于不整改的App采用强制下线来保证用户的权利。

[0003] 因此,需要对APP收集个人数据是否合规进行检测,以帮助APP上线隐私合规。

发明内容

[0004] 本申请的实施例提供一种应用程序的隐私合规检测方法,可针对不同的不合规问题类型创建检测分析模型,保证应用程序的隐私合规检测的针对性更强。

[0005] 为达到上述目的,本申请的实施例采用如下技术方案:

[0006] 第一方面,本申请公开了一种应用程序的隐私合规检测方法,检测方法包括:从不合规问题数据库中选择需检测的不合规问题类型,不合规问题数据库中存储多个不合规问题类型;获取待检测应用程序(application software,简称APP)的隐私声明文本;根据选择的需检测的不合规问题类型和待检测应用程序,确定合规的隐私数据集合;根据隐私声明文本和/或待检测应用程序的源码(即源代码),确定来自待检测应用程序的实际采集的隐私数据集合;根据合规的隐私数据集合和实际采集的隐私数据集合,确定待检测应用程序的隐私合规性。

[0007] 根据本申请的实施方式,可通过预先构建不合规问题数据库,从不合规问题数据库中选择需检测的不合规问题类型,根据所选择的不合规问题类型和待检测APP确定合规的隐私数据集合,根据隐私声明文本或者根据待检测应用程序的源码或者同时根据隐私声明文本以及待检测应用程序的源码确定实际采集的隐私数据集合;将合规的隐私数据集合和实际采集的隐私数据集合进行比对分析,确定待检测APP的隐私合规性,保证应用程序的隐私合规检测的针对性更强。若待检测APP存在隐私合规问题,则要求APP的运营方进行整改。若待检测APP不存在隐私合规问题,则APP可以发布。

[0008] 本申请基于不合规收集问题类型出发,保证系统的可扩展性,不合规问题数据库可以定期更新新增的不合规问题类型,有利于更全面地对待检测APP进行隐私合规检测。

[0009] 在上述第一方面的一种可能实现中,不合规问题类型包括:过度收集问题,过度收集问题是指实际采集的隐私数据集合超过了合规的隐私数据集合。可通过预先构建不合规问题数据库,将过度收集问题储存在不合规问题数据库中。通过检测应用程序是否存在过

度收集问题，从而可以确定应用程序是否收集了不应该收集的隐私数据。可以帮助应用程序运营方APP上线隐私合规，避免由于APP发布后不合规而要求下架或者受到处罚的风险。

[0010] 在上述第一方面的一种可能实现中，合规的隐私数据集合包括个人隐私数据集合，实际采集的隐私数据集合包括个人隐私数据集合和非个人隐私数据集合。通过隐私合规检测，确定应用程序是否存在隐私数据识别错误，即应用程序是否存在将非个人隐私数据和个人隐私数据一起收集的问题。其中，非个人隐私数据集合是不应该被收集的隐私数据。

[0011] 在上述第一方面的一种可能实现中，不合规问题类型包括：持续收集问题，持续收集问题是指隐私声明文本描述的内容和待检测应用程序所发布的国家或地区的标准文件不对应，标准文件由隐私合规监管机构颁布。可将持续收集问题储存在不合规问题数据库中。由于不同国家和地区对APP隐私声明的隐私法律法规往往是不一样的，理论上应该根据当地国家和地区的隐私法律法规相应地描述隐私声明。若在不同国家或地区发布的APP使用的是同一版本的隐私声明，就很有可能不符合当地国家或地区的隐私法律法规的规定。因此，通过检测应用程序是否存在持续收集问题，帮助应用程序运营方判断是否针对不同国家和地区相应地进行隐私描述。

[0012] 上述不合规问题类型是本申请的示例说明，本申请对此不做限制，实际还存在其它类型的不合规问题(例如隐私声明不符合监管规定的问题)。可以根据检测的大数据分析相应地储存在不合规问题数据库中，以便后续进行问题类型的选择。

[0013] 在上述第一方面的一种可能实现中，确定合规的隐私数据集合，包括：从预先采集的合规的隐私数据集合库中确定相对应的合规的隐私数据集合。即，可以预先建立一个合规的隐私数据集合库，合规的隐私数据结合库中会存储多个合规的隐私数据集合。合规的隐私数据集合库是预先存储。示例性地，可以通过大数据分析的方式预先采集合规的隐私数据集合。例如通过大数据分析了100款应用程序，确定市面上大部分的应用程序合规的隐私数据集合。即，可以预先采集更多的合规的隐私数据集合，使得待检测应用程序的隐私合规分析更加全面。

[0014] 在上述第一方面的一种可能实现中，确定合规的隐私数据集合，包括：通过扫描隐私声明文本确定合规的隐私数据集合。即，合规的隐私数据集合是通扫描隐私声明文本实时采集确定的。通过扫描隐私声明文本，确定合规的隐私数据集合，检测待检测应用程序采集的隐私数据是否和自身隐私声明文本描述的内容相一致，使得待检测应用程序的隐私合规分析更加精准和简单。

[0015] 在上述第一方面的一种可能实现中，通过扫描隐私声明文本确定合规的隐私数据集合，包括：通过扫描隐私声明文本声明的实现设定功能需采集的隐私数据集合确定为合规的隐私数据集合。这样可以确定待检测应用程序是否严格按照功能需求来合规收集隐私数据。若出现基于某功能收集了其他隐私数据，则待检测应用程序的隐私数据收集不合规，需要及时整改。

[0016] 在上述第一方面的一种可能实现中，确定合规的隐私数据集合，包括：获取需检测的不合规问题类型和待检测应用程序对应的标准文件，标准文件由隐私合规监管机构颁布；从标准文件中确定合规的隐私数据集合。在前述步骤实现方式中确定需检测的不合规问题类型和待检测应用程序后，根据需检测的不合规问题类型和待检测应用程序确定对应

的标准文件;然后再从标准文件中确定合规的隐私数据集合。从而,在前述隐私合规的检测过程的基础上,还增加了检测待检测应用程序隐私数据采集是否符合隐私合规监管机构颁布的标准文件的规定。使得待检测应用程序的隐私合规检测分析更加全面。

[0017] 在上述第一方面的一种可能实现中,确定来自待检测应用程序的实际采集的隐私数据集合,包括:扫描隐私声明文本;从隐私声明文本中获取待检测应用程序的功能和隐私数据的关联关系,确定待检测应用程序的功能和隐私数据的关联关系为实际采集的隐私数据集合。

[0018] 示例性地,在前述确定合规的隐私数据集合的过程中(可以从预先采集的合规的隐私数据集合库中确定),确定了市面上大部分的应用程序合规的隐私声明文本描述内容,这样无需扫描待检测应用程序的源码,只要扫描待检测应用程序的隐私声明文本的描述内容确定实际采集的隐私数据集合,就可以与合规的隐私数据集合进行比对分析,以确定待检测应用程序的隐私合规性。省去了扫描待检测应用程序的源码的过程,隐私合规检测过程简单。

[0019] 在上述第一方面的一种可能实现中,确定来自待检测应用程序的实际采集的隐私数据集合,包括:扫描待检测应用程序的源码;对源码进行解析,获取待检测应用程序的功能和隐私数据的关联关系,确定待检测应用程序的功能和隐私数据的关联关系为实际采集的隐私数据集合。通过扫描待检测应用程序的源代码,更精准地获取待检测应用程序的功能和隐私数据的关联关系,提升隐私合规检测的准确性。

[0020] 在上述第一方面的一种可能实现中,获取待检测应用程序的功能和隐私数据的关联关系,包括:对源码进行解析,获取待检测应用程序的功能、代码类和方法的对应关系;遍历待检测应用程序的功能,获取代码类和隐私数据的对应关系;根据待检测应用程序的功能、代码类和方法的对应关系,以及代码类和隐私数据的对应关系获取待检测应用程序的功能和隐私数据的关联关系。

[0021] 在上述第一方面的一种可能实现中,确定来自待检测应用程序的实际采集的隐私数据集合,包括:根据隐私声明文本,检测系统反馈信息和/或用户输入的信息;根据系统反馈信息和/或用户输入的信息,确定来自待检测应用程序的实际采集的隐私数据集合。

[0022] 即,通检测系统反馈信息,根据系统反馈信息确定来自待检测应用程序的实际采集的隐私数据集合。

[0023] 可以通过优化系统接口,针对获取系统数据的接口进行扩充,添加调用方信息(包名调用频率等)实现获取系统反馈信息。在系统层面做了改进,优化后的系统可以更加准确的确定待检测应用程序访问了哪些系统接口,以确定待检测应用程序的访问是否合规,保证检测准确性更高。

[0024] 或者,检测用户输入的信息(例如在用户输入个人隐私数据场景),根据用户输入的信息确定来自待检测应用程序的实际采集的隐私数据集合。同样也是在系统层面做了改进,可以对系统UI(User Interface,用户界面)控件进行优化。将监控UI控件中输入的有效数据,确定为应用程序实际采集的隐私数据集合。优化后的系统可以更加准确的帮助待检测应用程序检测使用的个人数据,保证检测准确性更高,实用性更强。

[0025] 或者,同时检测系统反馈信息和用户输入的信息,同时根据系统反馈信息以及用户输入的信息确定来自待检测应用程序的实际采集的隐私数据集合。

[0026] 在上述第一方面的一种可能实现中，方法还包括：检测待检测应用程序的网络请求，根据所检测的网络请求结果、合规的隐私数据集合和实际采集的隐私数据集合，确定待检测应用程序的隐私合规性。通过检测待检测应用程序是否进行了网络请求，判定待检测应用程序的隐私收集的风险性。在一些可能的实施方式中，标准文件规定应用程序不能进行网络请求。若根据检测的网络请求结果显示，待检测应用程序进行了网络请求，则存在隐私收集不合规的问题。通过检测待检测应用程序的网络请求，可以判定待检测应用程序的隐私收集的风险性。进一步提升隐私合规检测的全面性。

[0027] 第二方面，本申请的实施例公开了一种计算机可读存储介质，计算机可读存储介质上存储有指令，该指令在计算机上执行时使得计算机执行上述第一方面的检测方法。

附图说明

[0028] 图1根据本申请的一些实施例，示出了电子设备的用户界面示意图；

[0029] 图2根据本申请的一些实施例，示出了应用程序的隐私合规检测场景示意图；

[0030] 图3示出了本申请一个实施例提供的电子设备的框图；

[0031] 图4示出了本申请一个实施例提供的应用程序的隐私合规检测的流程图一；

[0032] 图5示出了本申请一个实施例提供的扩充获取系统数据的接口的示意图；

[0033] 图6示出了本申请一个实施例提供的检测用户输入的信息的流程图；

[0034] 图7示出了本申请一个实施例提供的应用程序的隐私合规检测的流程图二；

[0035] 图8示出了本申请一个实施例提供的应用程序的隐私合规检测的界面示意图；

[0036] 图9为本申请实施方式提供的隐私合规检测装置的构造示意图；

[0037] 图10为本申请实施方式提供的电子设备的构造示意图；

[0038] 图11示出了本申请一个实施例提供的一种片上系统(SoC)的框图。

具体实施方式

[0039] 以下将参考附图详细说明本申请的具体实施方式。

[0040] 本申请提供了一种应用程序的隐私合规检测方法，可针对不同的不合规问题类型创建检测分析模型，保证应用程序的隐私合规检测的针对性更强，分析问题更加精准。

[0041] App在使用和收集隐私数据时，通常都需要把使用和收集隐私数据的场景在应用程序的隐私声明中说明。APP不限于是安装于以手机10为示例的电子设备中的应用程序，电子设备也可以是笔记本电脑、平板电脑、超级移动个人计算机(ultra-mobile personal computer，UMPC)、手持计算机、上网本、个人数字助理(personal digital assistant，PDA)、可穿戴设备、虚拟现实设备等安装有应用程序的电子设备。

[0042] 示例性地，图1示出一个手机APP(例如荣耀商城)的一份隐私声明，这份隐私声明示例性地说明了该APP使用和收集隐私数据的场景，例如图1所示的：1、为您提供交易、服务、社区等相关功能或服务，我们会收集、使用您电话号码、身份证、地理位置、网络访问日志等必要信息；2、摄像头、麦克风、相册等敏感权限均不会默认开启，只有经过您明示授权的前提下才会实现某项功能或服务时使用；3、提供打电话功能需要获取设备序列号；4、在必要情况下，我们收集的您的信息会上传服务器。本申请对隐私声明描述的内容不做限制，根据APP实际开发的内容和功能等进行相应的隐私声明描述。

[0043] 当用户在隐私声明界面点击“同意”之后，才能正常使用该App。用户也可以通过App提供的查询界面随时查询隐私声明中的文本信息。这种方式都是为了保证App隐私合规。APP隐私合规可以是指APP运营方在APP使用过程中采集的隐私数据需要符合相关监管规定。也可以是指APP的隐私声明所描述的内容需要符合相关监管规定。

[0044] 上述的隐私数据包括个人隐私数据和非个人隐私数据。个人隐私数据可以是指与使用APP的个人相关的、不想被他人或无关人等获知的信息。通过个人隐私数据能够定位或识别个人的信息，个人隐私数据例如是电话号码、身份证、用户名、家庭地址、银行卡号、个人健康信息、个人就职单位、职位、个人文件、照片等数据。非个人隐私数据例如是使用的设备的相关信息(例如设备序列号)、用户使用APP过程中采集的道路交通信息等数据。

[0045] 但是由于开发人员隐私保护知识的匮乏、法律法规变化和隐私数据定义的变化等因素都会导致APP在收集隐私数据的过程中存在不合规收集的问题，并且APP不合规收集的问题类型较多，这些不合规问题将严重影响用户的隐私安全以及APP的正常使用(可能会被下架)。

[0046] 为此，本申请提供了一种应用程序的隐私合规检测方法，可通过预先构建不合规问题数据库，针对不同的不合规问题类型有针对性地创建合规检测分析模型，通过合规检测模型分析APP合规的隐私数据和APP实际采集的隐私数据，确定APP的隐私合规性，保证应用程序的隐私合规检测的针对性更强，分析问题更加精准。若APP存在隐私合规问题，则要求APP的运营方进行整改。若APP不存在隐私合规问题，则APP可以发布。

[0047] 在本申请的实施方式中，进行隐私合规检测的APP可以是新开发的APP，或者版本更新后的APP。在实际应用中，在新开发APP或者更新APP后，APP的运营方可以使用本申请的隐私合规检测方法检测APP是否隐私合规。在检测结果显示APP隐私合规之后，APP的运营方发布APP供用户使用。避免由于APP发布后不合规而要求下架或者受到处罚的风险。在一些可能的实施方式中，隐私监管机构或者应用发布平台也可以使用本申请的隐私合规检测方法进行APP的隐私合规检测。

[0048] 下面先示例性介绍不合规问题的几种类型。不合规问题的类型包括：

[0049] 1、过度收集问题。

[0050] 过度收集问题是指APP实现相应功能实际收集的隐私数据超过了APP隐私申明收集的隐私数据。包括过度收集个人隐私数据、过度收集非个人隐私数据以及同时过度收集个人隐私数据以及非个人隐私数据。

[0051] 例如，图1所示的隐私声明说明了“提供打电话功能需要获取设备序列号”，若APP提供打电话功能时，除了收集设备序列号，还收集了个人打电话的位置、时间等数据，这就出现了APP隐私申明收集的隐私数据(设备序列号)和APP实际收集的隐私数据(设备序列号和打电话的位置、时间等数据)不一致的问题。从而，APP提供打电话功能时，就存在过度收集隐私数据的问题，即APP过度收集了个人电话的位置、时间等个人隐私数据。

[0052] 又例如，在用户输入用户名登录用户的场景，隐私声明说明了用户在登录APP时会收集用户名和登录密码，这属于个人隐私数据。但当用户在登录APP时，APP不仅收集了用户名和登录密码，还收集了用户的身份证或设备序列号(非个人隐私数据)等隐私数据。APP就存在过度收集个人隐私数据和非个人隐私数据的问题。

[0053] 或者，图1所示的隐私声明没有说明要收集道路交通数据，但用户在使用APP的过

程中,APP却收集了道路交通数据。道路交通数据属于本申请所描述的非个人隐私数据,APP就存在过度收集非个人隐私数据的问题。

[0054] 2、持续收集问题。

[0055] 持续收集问题是指隐私声明描述的内容和APP所发布的国家或地区的标准文件不对应,标准文件由该国家或地区的隐私合规监管机构颁布。例如,APP在中国发布时用的是图1所示的隐私声明。当APP又在其它国家或地区(例如欧洲)发布时也使用的是图1所示的隐私声明。即,不同国家或地区发布的APP使用的是同一版本的隐私声明。

[0056] 而不同国家和地区对APP隐私声明的隐私法律法规往往是不一样的,理论上应该根据当地国家和地区的隐私法律法规相应地描述隐私声明。若在不同国家或地区发布的APP使用的是同一版本的隐私声明,就很有可能不符合当地国家或地区的隐私法律法规的规定。因此,APP就存在持续收集问题。

[0057] 3、隐私声明不符合监管规定的问题。

[0058] 其中,监管规定可以是指一些法律法规,例如《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《移动互联网应用程序信息服务管理规定》、GDPR(通用数据保护条例,General Data Protection Regulation)等法律法规。若APP的隐私声明描述的内容本身不符合这些法律规定,就存在隐私声明不符合监管规定的问题。

[0059] 例如,监管规定APP不得收集用户的身份证和地理位置等个人敏感隐私数据。但图1所示的隐私声明却描述了“我们会收集、使用您电话号码、身份证、地理位置、网络访问日志等必要信息”,那么隐私声明中描述的关于“收集身份证和地理位置”的内容就不符合监管规定。因此,APP就存在隐私声明不符合监管规定的问题。

[0060] 需说明的是,上述的三项不合规问题类型只是本申请的示例说明,实际还存在其它类型的不合规问题,在此不再列举。

[0061] 图2示出了运用本申请提供的应用程序合规检测的场景示意图。如图2所示,当需要对手机10中安装的APP进行隐私合规检测时,将手机10与隐私合规检测装置20(例如电脑)通过USB连接。在隐私合规检测过程中手机10和隐私合规检测装置20通过USB进行数据交换。但本申请对手机10和隐私合规检测装置20的连接方式不限于是通过USB的有线连接方式,在一些可能的实施方式中,可以是通过无线连接方式(例如“一碰传”方式)实现数据交换。

[0062] 在隐私合规检测过程中,上述的手机10将APP的相关数据(例如隐私声明文本和源码)上传给隐私合规检测装置20,隐私合规检测装置20读取APP的相关数据,获取APP的相关隐私数据,实现对APP的隐私合规检测。后文将详细说明应用程序的隐私合规检测过程。

[0063] 在如图2所示的场景中,笔记本电脑作为隐私合规检测装置20的本体的示例被提供。但是本申请不限于此,该电子设备的本体也可以是手机10、平板电脑、超级移动个人计算机(ultra-mobile personal computer,UMPC)、手持计算机、上网本、个人数字助理(personal digital assistant,PDA)、可穿戴设备、虚拟现实设备等安装有隐私合规检测程序的电子设备。

[0064] 现在参考图3,所示为根据本申请的一个实施例的电子设备400的框图。本申请隐私合规检测装置20的结构可以和电子设备400的结构相同。电子设备400可以包括耦合到控制器中枢403的一个或多个处理器401。对于至少一个实施例,控制器中枢403经由诸如前端

总线(FSB,Front Side Bus)之类的多分支总线、诸如快速通道连(QPI,QuickPath Interconnect)之类的点对点接口、或者类似的连接406与处理器401进行通信。处理器401执行控制一般类型的数据处理操作的指令。在一实施例中,控制器中枢403包括,但不局限于,图形存储器控制器中枢(GMCH,Graphics&Memory Controller Hub)(未示出)和输入/输出中枢(IOH,Input Output Hub)(其可以在分开的芯片上)(未示出),其中GMCH包括存储器和图形控制器并与IOH耦合。

[0065] 电子设备400还可包括耦合到控制器中枢403的协处理器402和存储器404。或者,存储器和GMCH中的一个或两者可以被集成在处理器内(如本申请中所描述的),存储器404和协处理器402直接耦合到处理器401以及控制器中枢403,控制器中枢403与IOH处于单个芯片中。

[0066] 存储器404可以是例如动态随机存取存储器(DRAM,Dynamic Random Access Memory)、相变存储器(PCM,Phase Change Memory)或这两者的组合。存储器404中可以包括用于存储数据和/或指令的一个或多个有形的、非暂时性计算机可读介质。计算机可读存储介质中存储有指令,具体而言,存储有该指令的暂时和永久副本。该指令可以包括:由处理器中的至少一个执行时导致电子设备400实施如后述图4所示方法的指令。当指令在计算机上运行时,使得计算机执行本申请实施例或组合实施例公开的方法。

[0067] 在一个实施例中,协处理器402是专用处理器,诸如例如高吞吐量MIC(Many Integrated Core,集成众核)处理器、网络或通信处理器、压缩引擎、图形处理器、GPGPU(General-purpose computing on graphics processing units,图形处理单元上的通用计算)、或嵌入式处理器等等。协处理器402的任选性质用虚线表示在图3中。

[0068] 在一个实施例中,电子设备400可以进一步包括网络接口(NIC,Network Interface Controller)406。网络接口406可以包括收发器,用于为电子设备400提供无线电接口,进而与任何其他合适的设备(如前端模块,天线等)进行通信。在各种实施例中,网络接口406可以与电子设备400的其他组件集成。网络接口406可以实现上述实施例中的通信单元的功能。

[0069] 电子设备400可以进一步包括输入/输出(I/O,Input/Output)设备405。I/O405可以包括:用户界面,该设计使得用户能够与电子设备400进行交互;外围组件接口的设计使得外围组件也能够与电子设备400交互;和/或传感器设计用于确定与电子设备400相关的环境条件和/或位置信息。

[0070] 值得注意的是,图3仅是示例性的。即虽然图3中示出了电子设备400包括处理器401、控制器中枢403、存储器404等多个器件,但是,在实际的应用中,使用本申请各方法的设备,可以仅包括电子设备400各器件中的一部分器件,例如,可以仅包含处理器401和网络接口406。图3中可选器件的性质用虚线示出。

[0071] 以下将结合附图详细阐述本申请实施例提供的一种应用程序的隐私合规检测方法,可通过预先构建不合规问题数据库,针对不同的不合规问题类型有针对性地创建合规检测分析模型,通过合规检测模型,并根据合规的隐私数据集合和实际采集的隐私数据集合,确定APP的隐私合规性,保证应用程序的隐私合规检测的针对性更强,分析问题更加精准。

[0072] 以下结合图4所示的流程图,详细介绍本申请应用程序的隐私合规检测方法。以下

待检测应用程序以荣耀商城为示例说明，但不限于是荣耀商城，还可以是其它应用程序，例如支付宝等。

[0073] 具体地，如图4所示，本实施例提供的方法包括以下步骤：

[0074] S100：从不合规问题数据库中选择需检测的不合规问题类型。

[0075] 现有APP不合规问题的类型有多种，例如前文所示例描述的过度收集问题、持续收集问题以及隐私声明不符合监管规定的问题。这些不合规问题类型会预先收集，并创建不合规问题数据库。不合规问题数据库例如存储的是不合规问题类型列表，如表1所示。通过对不合规问题进行分类，提供输入不合规问题的选择项。即，预先创建不合规问题数据库，在不合规问题数据中存储多个不合规问题类型。以便隐私合规检测人员在对APP进行合规检测时，从不合规问题数据中选择需检测的不合规问题类型。

[0076] 表1不合规问题数据库

[0077]

不合规问题类型
过度收集
持续收集
隐私声明不符合监管规定
……

[0078] 例如，隐私合规检测人员需要检测待检测的APP是否存在过度收集问题，那么就从不合规问题数据库的问题选项中(例如是列表中选择不合规问题类型)选择“过度收集”这个选项。从而，就可以对待检测APP进行是否存在“过度收集问题”的隐私合规检测。

[0079] 示例性地，上述不合规问题的来源包括外部来源和内部来源。其中，外部来源的不合规问题例如是工信部爆出的相关问题，此问题会带有固定的数据信息。后述的合规的隐私数据可以是工信部提供的这个固定的数据信息。内部来源的不合规问题例如是通过本方法扫描出来的典型问题，包括App自身存在问题和大数据分析出来的问题。

[0080] S200：获取待检测应用程序的隐私声明文本。

[0081] 上述S100所述描述的选择需检测的不合规问题类型是为应用程序隐私合规检测做准备。示例性地，在选择不合规问题类型之前或者之后，将荣耀商城的相关数据导入隐私合规检测装置20。隐私合规检测装置20从待检测应用程序中获取隐私声明文本。根据待检测应用程序的隐私声明文本的描述，可以获得待检测应用程序的功能，和实现相应的功能要获取的隐私数据。

[0082] 例如，隐私合规检测装置20获取了图1所示的应用程序的隐私声明，从而，可以获得荣耀商城的功能例如是提供交易、服务、打电话功能。其中，提供交易、服务功能需要收集用户的电话号码、身份证、地理位置和网络访问日志等个人隐私数据。而荣耀商城实现打电话功能要收集设备序列号这个非个人隐私数据。

[0083] S300：确定合规的隐私数据集合。

[0084] 合规的隐私数据集合是与需检测的不合规问题类型以及待检测应用程序相对应的，根据选择的需检测的不合规问题类型和待检测应用程序，就可以确定合规的隐私数据集合。合规的隐私数据集合是待检测应用程序收集隐私数据的正确标准，若待检测应用程序收集的隐私数据与这个合规的隐私数据集合不一致，就表明待检测应用程序存在隐私合规问题。其中，合规的隐私数据集合中数据可以是一个，也可以是一个以上。例如下表2示例

性的列出了应用程序实现的功能所收集的合规的隐私数据集合。

[0085] 表2合规的隐私数据集合表

[0086]

应用程序实现的功能	合规的隐私数据集合
交易、服务、社区	电话号码、身份证、地理位置、网络访问日志
打电话	设备序列号

[0087] 如表2所示，实现“交易、服务、社区”对应的合规的隐私数据集合包括是四个隐私数据：电话号码、身份证、地理位置以及网络访问日志。

[0088] 例如，待检测应用程序是荣耀商城，确定需检测的不合规问题类型是打电话是否存在过度收集问题。那么，检测荣耀商城是否存在实现“交易、服务、社区”功能过度收集问题，所对应的合规的隐私数据确定为：电话号码、身份证、地理位置和网络访问日志。那么，检测荣耀商城是否存在实现“打电话”功能过度收集问题，所对应的合规的隐私数据确定为：设备序列号。

[0089] 示例性的，合规的隐私数据集合可以从预先采集的合规的隐私数据集合库中确定。即，可以预先建立一个合规的隐私数据集合库，合规的隐私数据结合库中会存储多个合规的隐私数据集合。合规的隐私数据集合库是预先存储在隐私合规检测装置20中的，在确定了需检测的不合规问题类型(例如过度收集问题)和待检测应用程序(例如荣耀商城)后，相对应的合规的隐私数据集合就确定了。

[0090] 示例性地，可以通过大数据分析的方式预先采集合规的隐私数据集合。例如通过大数据分析了100款应用程序，获得这些应用程序的隐私声明在描述实现“打电话”功能时收集的隐私数据都是：获取设备序列号。从而，可以将实现“打电话”功能对应收集的隐私数据(获取设备序列号)确定为合规的隐私数据集合。通过对不同功能对应收集的隐私数据进行大数据分析，可以构建隐私数据集合库。

[0091] 示例性的，合规的隐私数据集合可以通过扫描待检测应用程序的隐私声明文本确定合规的隐私数据集合。即，合规的隐私数据集合是实时采集确定的。例如，隐私合规检测装置20通过扫描荣耀商城的隐私声明文本确定了“打电话”功能需要收集的隐私数据是：获取设备序列号。那么，隐私合规检测装置20在扫描荣耀商城的隐私声明文本后，就将实现“打电话”功能对应收集的隐私数据(获取设备序列号)确定为合规的隐私数据集合。

[0092] 示例性的，合规的隐私数据集合是从前文所描述的标准文件中确定的。在前述步骤确定了需检测的不合规问题类型和待检测应用程序后，隐私合规检测装置20会根据需检测的不合规问题类型和待检测应用程序确定对应的标准文件；然后隐私合规检测装置20再从标准文件中确定合规的隐私数据集合。

[0093] 例如，确定需检测的不合规问题类型是过度收集问题，待检测应用程序是荣耀商城。那么对应的标准文件是《中华人民共和国国家安全法》和《中华人民共和国网络安全法》。对应的标准文件确定合规的隐私数据集合例如是下表3所示：

[0094] 表3标准文件的合规的隐私数据集合

[0095]

应用程序实现的功能	合规的隐私数据集合
交易、服务、社区	电话号码、网络访问日志
打电话	设备序列号
……	……

[0096] 如表3所示，标准文件确定的实现“交易、服务、社区”功能对应的合规的隐私数据集合包括是一个隐私数据：电话号码和网络访问日志。标准文件确定的实现“打电话”功能对应的合规的隐私数据集合包括一个隐私数据：设备序列号。

[0097] S400：确定来自待检测应用程序的实际采集的隐私数据集合。

[0098] 对于待检测应用程序实际采集的隐私数据集合可以通过应用程序的扫描隐私文本获取，或者扫描应用程序的源码获取。

[0099] 先描述通过扫描隐私文本确定实际采集的隐私数据集合的方式。示例性的，在一些可能的实施方式中，隐私合规检测装置20通过扫描图1所示的荣耀商城的隐私声明文本；从荣耀商城的隐私声明文本中获取荣耀商城的功能和隐私数据的关联关系。再确定荣耀商城的功能和隐私数据的关联关系为实际采集的隐私数据集合。表2示出了荣耀商城的功能和隐私数据的关联关系，确定隐私声明实现“交易、服务、社区”功能实际采集的隐私数据集合为：电话号码、身份证、地理位置和网络访问日志。以及实现“打电话”功能实际采集的隐私数据集合为：设备序列号。

[0100] 下面描述通过扫描应用程序的源码确定实际采集的隐私数据集合的方式。示例性地，隐私合规检测装置20通过扫描荣耀商城的源码；对荣耀商城的源码进行解析，获取荣耀商城的功能和隐私数据的关联关系，确定荣耀商城的功能和隐私数据的关联关系为实际采集的隐私数据集合。

[0101] 在一些可能的实施方式中，确定来自待检测应用程序的实际采集的隐私数据集合的方式还包括：隐私合规检测装置20检测系统反馈信息，隐私合规检测装置20根据系统反馈信息，确定来自待检测应用程序的实际采集的隐私数据集合。通过这一方法，隐私合规检测装置20可以确定待检测应用程序访问了哪些系统接口。以确定待检测应用程序的访问是否合规。

[0102] 例如，图1所示的隐私声明描述了实现“打电话”功能需要获取设备序列号。隐私合规检测装置20根据系统的反馈信息确定待检测应用程序访问了设备序列号接口。从而，隐私合规检测装置20确定待检测应用程序获取了设备序列号。若根据系统的反馈信息确定待检测应用程序不仅访问了设备的序列号接口，还访问了其它系统接口(例如耳机接口)，这表明待检测应用程序可能开启了麦克风。那么根据系统反馈的信息确定荣耀商城实现打电话功能实际采集的隐私数据集合为：设备序列号和麦克风。

[0103] 可以通过优化系统接口，针对获取系统数据的接口进行扩充，添加调用方信息(包名调用频率等)实现获取系统反馈信息。示例性的，如图5所示，关于扩充系统接口(getSn)的具体系统代码可以如下：public int getSn(){扩展方法(获取调用堆栈，堆栈中包含包名，类名，方法名)，添加调用频率原始代码}。将上述代码存储在数据中，实现扩充系统接口(getSn)

[0104] 在一些可能的实施方式中，确定来自待检测应用程序的实际采集的隐私数据集合的方式还包括：隐私合规检测装置20检测用户输入的信息，根据用户输入的信息，确定来自待检测应用程序的实际采集的隐私数据集合。示例性地，在用户输入个人隐私数据场景，在待检测应用程序的登录视图界面，用户输入用户名和登录密码。从而，待检测应用程序实际采集的隐私数据集合是：用户名和登录密码。示例性的，可以对系统UI(User Interface，用户界面)控件进行优化。将监控UI控件中输入的有效数据，确定为应用程序实际采集的隐私

数据集合。

[0105] 示例性地，如图6所示，用户在视图界面输入数据，系统会检查输入数据的类型，并检测用户输入的数据是否是有效的个人数据，检测方式例如是利用正则表达式确定用户输入的数据是否是有效的个人数据；在确定用户输入的数据类型是有效的个人数据，会将有效的个人数据存入数据库，否则不会出入数据库。从而，确定用户输入的有效的个人数据为实际采集的隐私数据集合。即确定用户数据映射关系是：确定了实现登录功能对应的用户名和登录密码。

[0106] 例如，登录密码是六位阿拉伯数字(123456)，监控UI控件时发现用户输入的密码是字母(abcdef)，不是六位阿拉伯数字，这不是有效的个人数据，系统不会将字母确定为用户输入的密码，也就不会确定为实际采集的隐私数据。只有监控UI控件时发现用户输入的是六位阿拉伯数字(123456)，确定用户输入的是有效的个人数据，从而确定为实际采集的隐私数据。

[0107] 在一些可能的实施方式中，隐私合规检测装置20根据系统反馈信息和用户输入的信息，确定来自待检测应用程序的实际采集的隐私数据集合。

[0108] S500：根据合规的隐私数据集合和实际采集的隐私数据集合，确定待检测应用程序的隐私合规性。

[0109] 在使用前述步骤S300中任一方式确定合规的隐私数据集合以及使用前述步骤S400中任一方式确定实际采集的隐私数据集合后，隐私合规检测装置20根据选择需检测的不合规问题类型对这两个隐私数据集合进行比对分析。确定待检测应用程序的隐私合规性。

[0110] 示例性地，参考图7，以确定需检测的不合规问题类型是荣耀商城打电话是否存在过度收集问题为示例说明本申请的合规检测过程。

[0111] 首先，从不合规问题数据库中选择需检测的不合规问题类型为：过度收集问题，并在隐私合规检测装置20中输入上述问题类型。

[0112] 接着，向隐私合规检测装置20导入荣耀商城。

[0113] 然后，分别确定荣耀商城实现打电话功能对应的合规的隐私数据集合和收集采集的隐私数据集合。

[0114] 对于确定合规的隐私数据的集合的方式是，扫描荣耀商城的隐私声明获取打电话功能和隐私数据的映射关系：打电话功能需要获取设备序列号。将此确定为荣耀商城打电话功能对应的合规的隐私数据集合，即图7中①所示。

[0115] 对于确定实际采集的隐私数据的集合的方式是，扫描荣耀商城的代码，获取荣耀商城的功能、代码类和方法的对应关系；遍历待荣耀商城的功能，获取代码类和隐私数据的对应关系。

[0116] 其中，参考图7，上述荣耀商城的功能、代码类和方法的对应关系如下所示：

[0117] 功能：打电话；

[0118] class：phone；

[0119] method：getphone{}getphone。

[0120] 参考图7，上述荣耀商城的代码类和隐私数据的对应关系如下所示：

[0121] 系统getSn；

[0122] 扩展的方法获取；

[0123] phone->getphone。

[0124] 根据荣耀商城的功能、代码类和方法的对应关系，以及代码类和隐私数据的对应关系获取荣耀商城的功能和隐私数据的关系如下：功能：打电话->getSn(获取设备序列号)。即，荣耀商城实现打电话功能实际采集的隐私数据集合为：设备序列号。将此确定为荣耀商城打电话功能实际采集的隐私数据集合，即图7中②所示。

[0125] 最后，将上述的合规的隐私数据集合(图7中①所示)和实际采集的隐私数据集合(图7中②所示)进行对比分析。

[0126] 若合规的隐私数据集合和实际采集的隐私数据集合完全一致，则不存在过度收集问题，荣耀商城的隐私数据收集合规，荣耀商城可以发布。

[0127] 反之，若根据前文步骤S400所描述的，实现“打电话”功能实际采集的隐私数据集合为：设备序列号和麦克风。则，荣耀商城实现打电话功能合规的隐私数据集合和实际采集的隐私数据集合是不一致的，荣耀商城实现打电话功能过度收集了隐私数据：麦克风。因此，荣耀商城的隐私数据收集不合规，需要整改。

[0128] 示例性地，参考图8，隐私合规检测装置20的检测界面上生成了一份隐私合规检测报告，报告显示合规的隐私数据和实际采集的隐私数据是一致的。从而，隐私合规检测报告的结论是：不存在过度收集问题。

[0129] 同样，可以选择其它不合规问题类型进行待检测应用程序进行隐私合规检测。

[0130] 在一些可能的实施方式中，上述的隐私合规检测方法还包括：检测待检测应用程序的网络请求，根据所检测的网络请求结果、合规的隐私数据集合和实际采集的隐私数据集合，确定待检测应用程序的隐私合规性。即，隐私合规检测装置20会检测待检测应用程序是否进行了网络请求，例如是待检测应用程序将实际采集的隐私数据集合是否上传了服务器。

[0131] 图1的隐私声明示出了“在必要情况下，我们收集的您的信息会上传服务器”。若待检测应用程序进行了网络请求，即将实际采集的隐私数据集合上传了服务器。虽然，隐私声明和实际采集的隐私数据集合一致，但是根据标准文件确定的合规的隐私数据集合规定隐私数据集合不得上传服务器。那么，待检测的隐私程序的隐私数据收集不合规。

[0132] 因此，通过检测待检测应用程序的网络请求，也可以判定待检测应用程序的隐私收集的风险性。

[0133] 综上，本申请基于不合规收集隐私数据问题类型出发，更加准确地保证系统的可扩展性，有利于后期新增问题分析；针对不同问题的类型创建不同的隐私合规检测模型，保证分析问题的针对性更强，分析问题更加精准。同时，在系统层面做了改进，优化后的系统可以更加准确的帮助App检测使用的隐私数据，保证检测准确性更高，实用性更强；本申请也可以解决APP代码中无法检测的场景。

[0134] 现在参考图9，所示为根据本申请的一个实施例的隐私合规检测装置20的框图。隐私合规检测装置20包括合规性分析模块111、不合规问题数据管理模块112、隐私声明读取模块113、代码扫描模块114、系统数据检测模块115以及用户输入个人数据检测模块116。其中，示例性地，不合规问题数据管理模块112用于执行S100，对前述不合规问题类型进行分类，提供输入不合规问题的选择项，创建不合规问题数据库；或者执行S300，用于提供合规

的隐私数据集合。示例性地，合规性分析模块111用于执行S500，根据选择的不合规问题的类型创建合规分析模型，对待检测应用程序进行隐私合规性分析。示例性地，隐私声明读取模块113用于执行S200；或者执行S300，以确定合规的隐私数据集合。示例性地，代码扫描模块114、系统数据检测模块115以及用户输入个人数据检测模块116用于执行S400。其中，系统检测模块115可以检测系统反馈信息。用户输入个人数据检测模块116可以检测用户输入的信息。

[0135] 图10示出了根据本申请一实施例的电子设备100的结构示意图。上述实施例中的手机10的结构和隐私合规检测装置20的结构可以与该电子设备100相同。具体地：

[0136] 电子设备100可以包括处理器110，外部存储器接口120，内部存储器121，通用串行总线(universal serial bus，USB)接头130，充电管理模块140，电源管理模块141，电池142，天线1，天线2，移动通信模块150，无线通信模块160，音频模块170，扬声器170A，受话器170B，麦克风170C，耳机接口170D，传感器模块180，按键190，马达191，指示器192，摄像头193，显示屏194，以及用户标识模块(subscriber identification module，SIM)卡接口195等。其中传感器模块180可以包括压力传感器180A，陀螺仪传感器180B，气压传感器180C，磁传感器180D，加速度传感器180E，距离传感器180F，接近光传感器180G，指纹传感器180H，温度传感器180J，触摸传感器180K，环境光传感器180L，骨传导传感器180M等。

[0137] 可以理解的是，本申请实施例示意的结构并不构成对电子设备100的具体限定。在本申请另一些实施例中，电子设备100可以包括比图示更多或更少的部件，或者组合某些部件，或者拆分某些部件，或者不同的部件布置。图示的部件可以以硬件，软件或软件和硬件的组合实现。

[0138] 处理器110可以包括一个或多个处理单元，例如：处理器110可以包括应用处理器(application processor，AP)，调制解调处理器，图形处理器(graphics processing unit，GPU)，图像信号处理器(image signal processor，ISP)，控制器，视频编解码器，数字信号处理器(digital signal processor，DSP)，基带处理器，和/或神经网络处理器(neural-network processing unit，NPU)等。其中，不同的处理单元可以是独立的器件，也可以集成在一个或多个处理器中。

[0139] 处理器可以根据指令操作码和时序信号，产生操作控制信号，完成取指令和执行指令的控制。

[0140] 处理器110中还可以设置存储器，用于存储指令和数据。在一些实施例中，处理器110中的存储器为高速缓冲存储器。该存储器可以保存处理器110刚用过或循环使用的指令或数据。如果处理器110需要再次使用该指令或数据，可从存储器中直接调用。避免了重复存取，减少了处理器110的等待时间，因而提高了系统的效率。

[0141] 在一些实施例中，处理器110可以包括一个或多个接口。接口可以包括集成电路(inter-integrated circuit，I2C)接口，集成电路内置音频(inter-integrated circuit sound，I2S)接口，脉冲编码调制(pulse code modulation，PCM)接口，通用异步收发传输器(universal asynchronous receiver/transmitter，UART)接口，移动产业处理器接口(mobile industry processor interface，MIPI)，通用输入输出(general-purpose input/output，GPIO)接口，用户标识模块(subscriber identity module，SIM)接口。

[0142] 外部存储器接口120可以用于连接外部存储卡，例如Micro SD卡，实现扩展电子设

备100的存储能力。外部存储卡通过外部存储器接口120与处理器110通信,实现数据存储功能。例如将音乐,视频等文件保存在外部存储卡中。

[0143] 内部存储器121可以用于存储计算机可执行程序代码,可执行程序代码包括指令。内部存储器121可以包括存储程序区和存储数据区。其中,存储程序区可存储操作系统,至少一个功能所需的应用程序(比如声音播放功能,图像播放功能等)等。存储数据区可存储电子设备100使用过程中所创建的数据(比如音频数据,电话本等)等。此外,内部存储器121可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件,闪存器件,通用闪存存储器(universal flash storage,UFS)等。处理器110通过运行存储在内部存储器121的指令,和/或存储在设置于处理器中的存储器的指令,执行电子设备100的各种功能应用以及数据处理。本实施例中,内部存储器121中存储有指令,该指令由处理器110执行时可使得电子设备100执行本申请实施方式提供的应用程序的隐私合规检测的方法。

[0144] 压力传感器180A用于感受压力信号,可以将压力信号转换成电信号。在一些实施例中,压力传感器180A可以设置于显示屏194,显示屏194例如是内折叠手机10的外屏11和内屏12,外折叠手机10的左屏13和右屏14。压力传感器180A的种类很多,如电阻式压力传感器,电感式压力传感器,电容式压力传感器等。电容式压力传感器可以是包括至少两个具有导电材料的平行板。当有力作用于压力传感器180A,电极之间的电容改变。电子设备100根据电容的变化确定压力的强度。当有触摸操作作用于显示屏194,电子设备100根据压力传感器180A检测所述触摸操作强度。电子设备100也可以根据压力传感器180A的检测信号计算触摸的位置。在一些实施例中,作用于相同触摸位置,但不同触摸操作强度的触摸操作,可以对应不同的操作指令。例如:当有触摸操作强度小于第一压力阈值的触摸操作作用于短消息应用图标时,执行查看短消息的指令。当有触摸操作强度大于或等于第一压力阈值的触摸操作作用于短消息应用图标时,执行新建短消息的指令。

[0145] 指纹传感器180H用于采集指纹。电子设备100可以利用采集的指纹特性实现指纹解锁,访问应用锁,指纹拍照,指纹接听来电等。

[0146] 触摸传感器180K,也称“触控器件”。触摸传感器180K可以设置于显示屏194,由触摸传感器180K与显示屏194组成触摸屏,也称“触控屏”。触摸传感器180K用于检测作用于其上或附近的触摸操作。触摸传感器可以将检测到的触摸操作传递给应用处理器,以确定触摸事件类型。可以通过显示屏194提供与触摸操作相关的视觉输出。在另一些实施例中,触摸传感器180K也可以设置于电子设备100的表面,与显示屏194所处的位置不同。

[0147] 现在参考图11,所示为根据本申请的一实施例的SoC(System on Chip,片上系统)500的框图。在图11中,相似的部件具有同样的附图标记。另外,虚线框是更先进的SoC的可选特征。在图11中,SoC500包括:互连单元550,其被耦合至处理器510;系统代理单元580;总线控制器单元590;集成存储器控制器单元540;一组或一个或多个协处理器520,其可包括集成图形逻辑、图像处理器、音频处理器和视频处理器;静态随机存取存储器(SRAM,Static Random-Access Memory)单元530;直接存储器存取(DMA,Direct Memory Access)单元560。在一个实施例中,协处理器520包括专用处理器,诸如例如网络或通信处理器、压缩引擎、GPGPU(General-purpose computing on graphics processing units,图形处理单元上的通用计算)、高吞吐量MIC处理器、或嵌入式处理器等。

[0148] 静态随机存取存储器(SRAM)单元530可以包括用于存储数据和/或指令的一个或多个有形的、非暂时性计算机可读介质。计算机可读存储介质中存储有指令，具体而言，存储有该指令的暂时和永久副本。该指令可以包括：由处理器中的至少一个执行时导致SoC实施如图4所示方法的指令。当指令在计算机上运行时，使得计算机执行上述实施例中公开的方法。

[0149] 本申请的各方法实施方式均可以以软件、磁件、固件等方式实现。

[0150] 可将程序代码应用于输入指令，以执行本文描述的各功能并生成输出信息。可以按已知方式将输出信息应用于一个或多个输出设备。为了本申请的目的，处理系统包括具有诸如例如数字信号处理器(DSP,Digital Signal Processor)、微控制器、专用集成电路(ASIC)或微处理器之类的处理器的任何系统。

[0151] 程序代码可以用高级程序化语言或面向对象的编程语言来实现，以便与处理系统通信。在需要时，也可用汇编语言或机器语言来实现程序代码。事实上，本文中描述的机制不限于任何特定编程语言的范围。在任一情形下，该语言可以是编译语言或解释语言。

[0152] 至少一个实施例的一个或多个方面可以由存储在计算机可读存储介质上的表示性指令来实现，指令表示处理器中的各种逻辑，指令在被机器读取时使得该机器制作用于执行本文的技术的逻辑。被称为“IP(Intellectual Property,知识产权)核”的这些表示可以被存储在有形的计算机可读存储介质上，并被提供给多个客户或生产设施以加载到实际制造该逻辑或处理器的制造机器中。

[0153] 在一些情况下，指令转换器可用来将指令从源指令集转换至目标指令集。例如，指令转换器可以变换(例如使用静态二进制变换、包括动态编译的动态二进制变换)、变形、仿真或以其它方式将指令转换成将由核来处理的一个或多个其它指令。指令转换器可以用软件、硬件、固件、或其组合实现。指令转换器可以在处理器上、在处理器外、或者部分在处理器上且部分在处理器外。

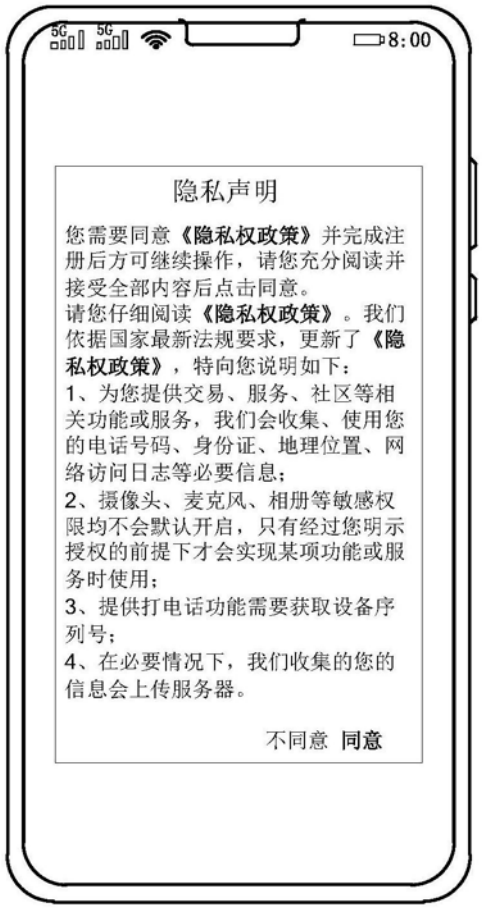

8:00
隐私声明
您需要同意《隐私权政策》并完成注册后方可继续操作，请您充分阅读并接受全部内容后点击同意。
请您仔细阅读《隐私权政策》。我们依据国家最新法规要求，更新了《隐私权政策》，特向您说明如下：
1、为您提供交易、服务、社区等相关功能或服务，我们会收集、使用您的电话号码、身份证、地理位置、网络访问日志等必要信息；
2、摄像头、麦克风、相册等敏感权限均不会默认开启，只有经过您明示授权的前提下才会实现某项功能或服务时使用；
3、提供打电话功能需要获取设备序列号；
4、在必要情况下，我们收集的您的信息会上传服务器。
不同意 同意

图1

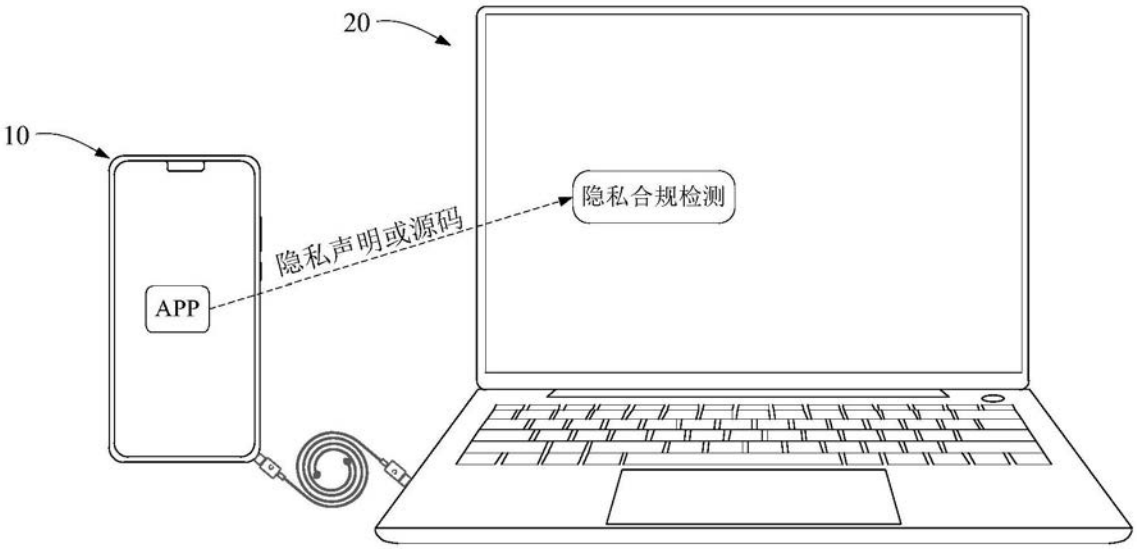

20
10
隐私合规检测
隐私声明或源码
APP

图2

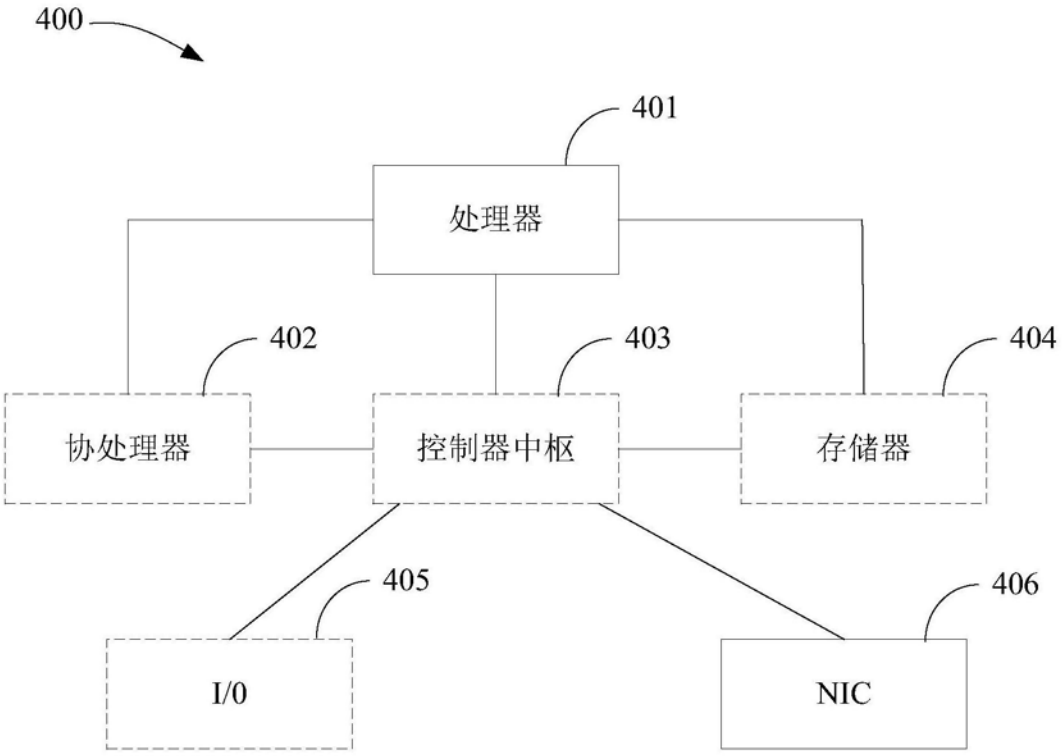


图3

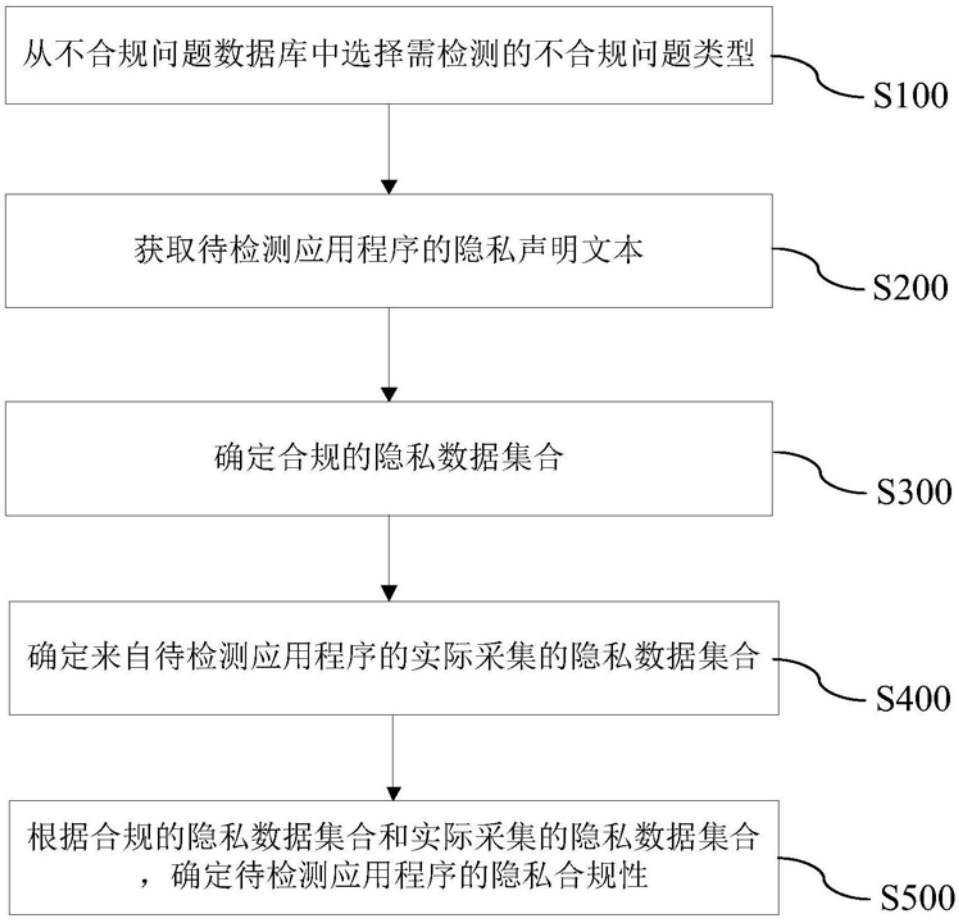

从不合规问题数据库中选择需检测的不合规问题类型
S100
获取待检测应用程序的隐私声明文本
S200
确定合规的隐私数据集合
S300
确定来自待检测应用程序的实际采集的隐私数据集合
S400
根据合规的隐私数据集合和实际采集的隐私数据集合，确定待检测应用程序的隐私合规性
S500

图4


系统接口（getSn）
public int getSn() { 扩展方法（获取调用堆栈，堆栈中包含包名，类名，方法名），添加调用频率 原始代码 }
存储数据库

图5


视图（View）
检查输入数据的类型
检测
是否是个人有效数据
存入数据库
用户数据映射关系

图6

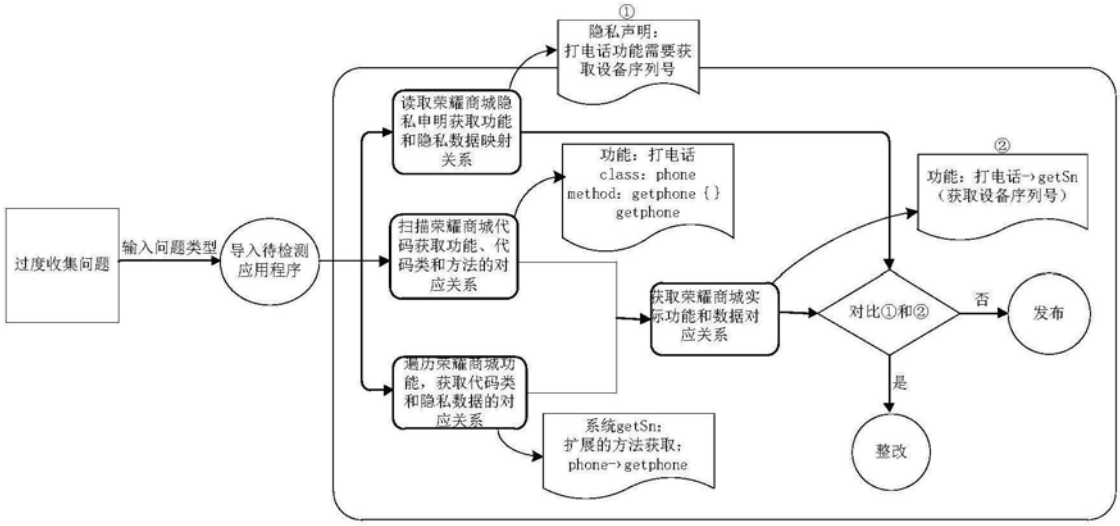

过度收集问题
输入问题类型
导入待检测应用程序
读取荣耀商城隐私申明获取功能和隐私数据映射关系
扫描荣耀商城代码获取功能、代码类和方法的对应关系
遍历荣耀商城功能，获取代码类和隐私数据的对应关系
①
隐私声明：打电话功能需要获取设备序列号
功能：打电话
class：phone
method：getphone｛｝
getphone
系统getSn：扩展的方法获取：phone→getphone
获取荣耀商城实际功能和数据对应关系
②
功能：打电话→getSn（获取设备序列号）
对比①和②
否
发布
是
整改

图7


20
隐私合规检测报告
问题类型：过度收集
合规隐私数据：打电话功能需收集设备序列号
实际采集的隐私数据：打电话功能收集了设备序列号
结论：不存在过度收集问题

图8

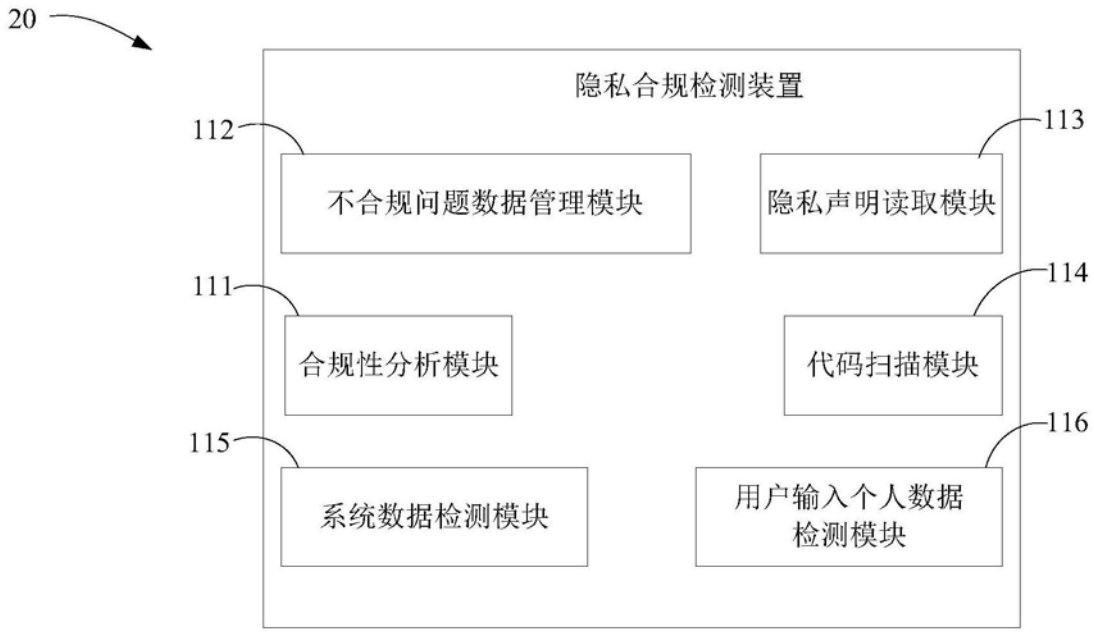

20
隐私合规检测装置
112
不合规问题数据管理模块
113
隐私声明读取模块
111
合规性分析模块
114
代码扫描模块
115
系统数据检测模块
116
用户输入个人数据
检测模块

图9

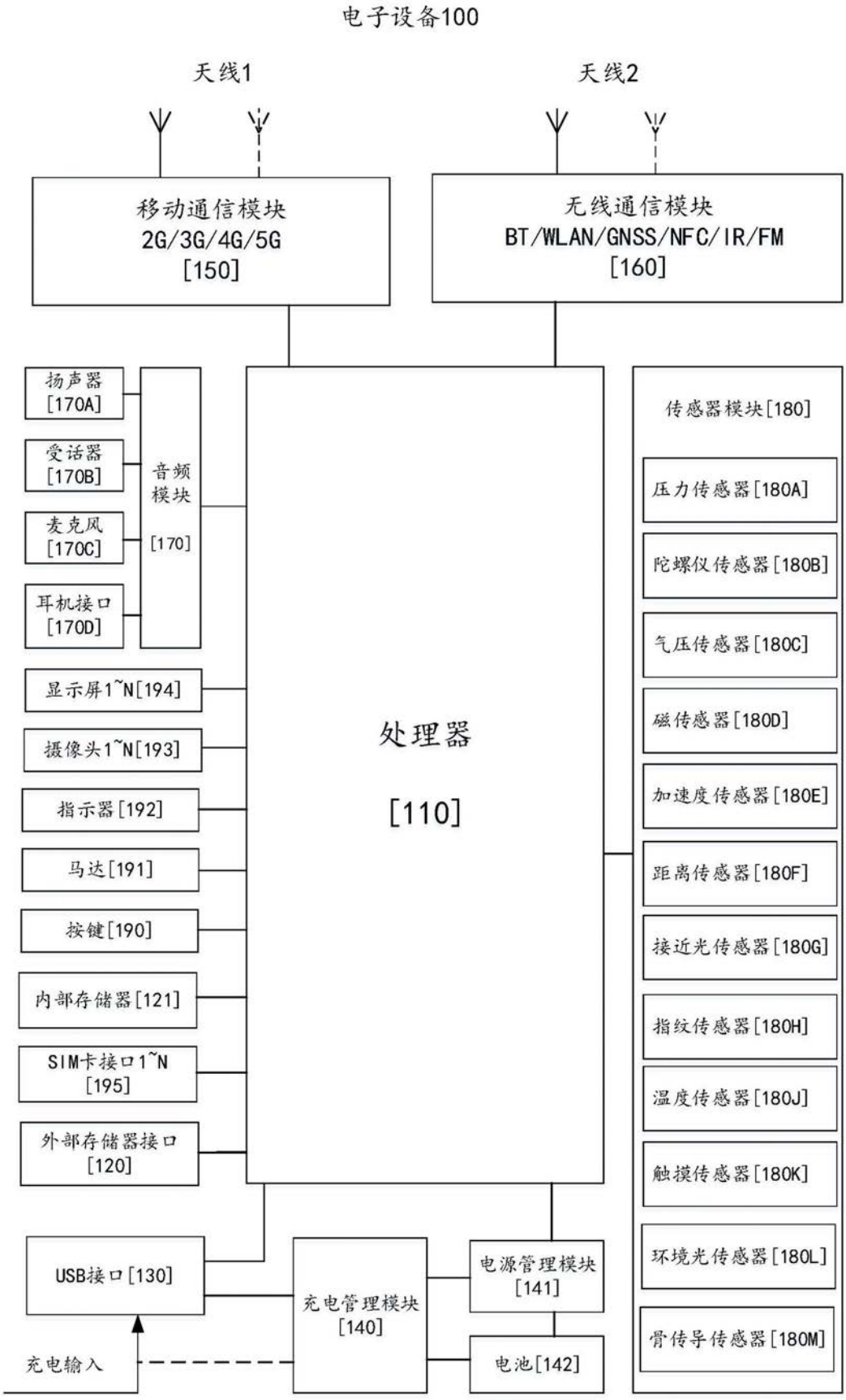

电子设备100
天线1
天线2
移动通信模块
2G/3G/4G/5G
[150]
无线通信模块
BT/WLAN/GNSS/NFC/IR/FM
[160]
扬声器
[170A]
受话器
[170B]
麦克风
[170C]
耳机接口
[170D]
音频
模块
[170]
显示屏1~N[194]
摄像头1~N[193]
指示器[192]
马达[191]
按键[190]
内部存储器[121]
SIM卡接口1~N
[195]
外部存储器接口
[120]
处理器
[110]
传感器模块[180]
压力传感器[180A]
陀螺仪传感器[180B]
气压传感器[180C]
磁传感器[180D]
加速度传感器[180E]
距离传感器[180F]
接近光传感器[180G]
指纹传感器[180H]
温度传感器[180J]
触摸传感器[180K]
环境光传感器[180L]
骨传导传感器[180M]
USB接口[130]
充电管理模块
[140]
电源管理模块
[141]
电池[142]
充电输入

图10

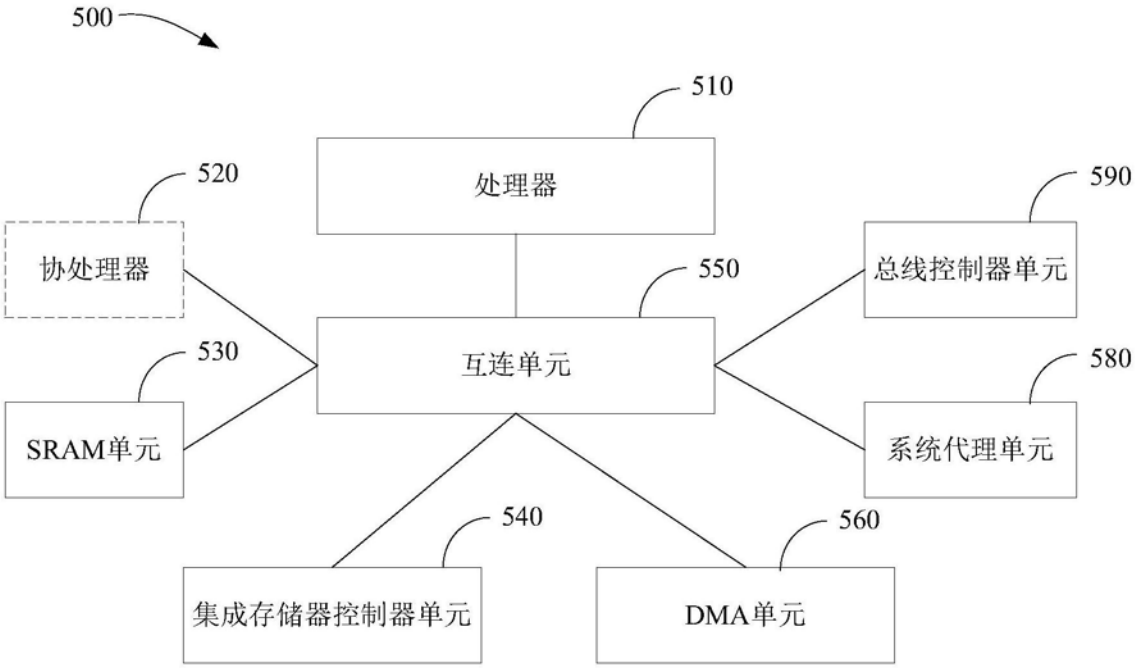

500
510
处理器
520
协处理器
590
总线控制器单元
550
互连单元
530
SRAM单元
580
系统代理单元
540
集成存储器控制器单元
560
DMA单元

图11