November 2020

# Automatic Reporting of Smartphone Privacy Risks

N/A

# Automatic Reporting of Smartphone Privacy Risks

**Abstract:**

This publication describes techniques for the automatic reporting of privacy risks detected on a computing device to a user. Some risks may include content collected and shared by physical sensors (e.g., camera, microphone, location, activity sensors) with applications installed on a computing device. These applications may use information from the sensors to perform operations for the user (e.g., providing directions on a map application, sharing a photo on a social media application, reporting on the health of a user). A user may opt in to a Privacy Manager to help detect risks by ranking content collected by applications, for example, in terms of perceived risk (e.g., sensitivity) to the user. The Privacy Manager may send automatic reports to the user with additional details and/or advise action to be taken if needed (e.g., disable the permissions granted to the application).

**Keywords:**

Automatic report, notification, privacy, security, automatic security, permissions, disable, monitor privacy, control privacy, security notification, confidential, privacy risk, security risk, application permissions, data

**Background:**

There is a growing concern among users to protect their privacy. Some users spend significant portions of their day using computing device applications (e.g., ride-share, movie streaming, social media) that utilize information received from physical sensors (e.g., camera,

microphone, location) of the device. The information obtained from physical sensors of a device (e.g., smartphone) can be considered confidential, causing some users to become concerned about their privacy. In an example, a user might use a ride-share application to travel to the airport, and that application may require permission from the user to access certain information to complete the task (e.g., location, text input of a credit card number). While the user may approve sharing information to complete the task, they may not want their information accessible by the application after arriving at the airport. Even though a user may opt in to an application on their computing device that requires information from physical sensors or input from the user (e.g., a photograph, text, audio dictation), it is not always obvious, for example, what data is being collected and stored by an application.

**Description:**

This publication describes techniques for the automatic reporting of privacy risks (e.g., security risks) detected on a computing device to a user. These risks may include information collected from physical sensors to allow for the operations of an application. For example, a navigation application may require permission from the user to access their location, or a social media application may require permission to access a camera on the computing device to allow the user to take a photo for a post.

While the example computing device described in this publication is a smartphone, other types of computing devices can also support the techniques described herein. A computing device may include one or more processors, transceivers for transmitting data to and receiving data from a base station (e.g., wireless access point, another computing device), sensors (e.g., a location sensor, an image sensor), a computer-readable medium (CRM), and/or an input/output device (e.g.,

a display, a speaker, a microphone). The CRM may include any suitable memory or storage device like random-access memory (RAM), static RAM (SRAM), dynamic RAM (DRAM), non-volatile RAM (NVRAM), read-only memory (ROM), or flash memory. The CRM includes device data (e.g., user data, multimedia data, applications, and/or an operating system of the device), which are executable by the processor(s) to enable the techniques described herein. The device data may include a Privacy Manager. The computing device performs operations under the direction of the Privacy Manager to detect if information from physical sensors is being accessed and/or stored by applications and to automatically report privacy risks to the user.

A user may be provided with controls allowing the user to make an election as to both if and when systems, applications, and/or features described herein may enable collection of user information (e.g., photos taken with the computing device camera, audio dictations, typed text, information about the social network of a user, online browsing history, application preferences, current location) and if the user is sent content and/or communications from a server. In addition, certain data may be treated in one or more ways before it is stored and/or used so that personally identifiable information is removed. For example, the geographic location of the user may be generalized where location information is obtained (e.g., to a city, ZIP code, or state level), so that a precise location of a user cannot be determined. Thus, the user may have control over what information is collected, how that information is used, and what information is provided to their computing device.

Some computing device applications require information from physical sensors to complete tasks. As illustrated in Figure 1, for example, a user may need to use a ride-share application to arrange travel to an airport with friends, and the application may ask the user for permission to access physical sensors on the computing device (e.g., to determine the location of

the user). Once the application determines the location of the user, for example, a driver can be sent to pick up the user and friends. Even though the user granted permission to the ride-share application to access sensors on the computing device, the user may want to know what information was collected, if the information is being stored, and if the information should be considered a privacy risk.

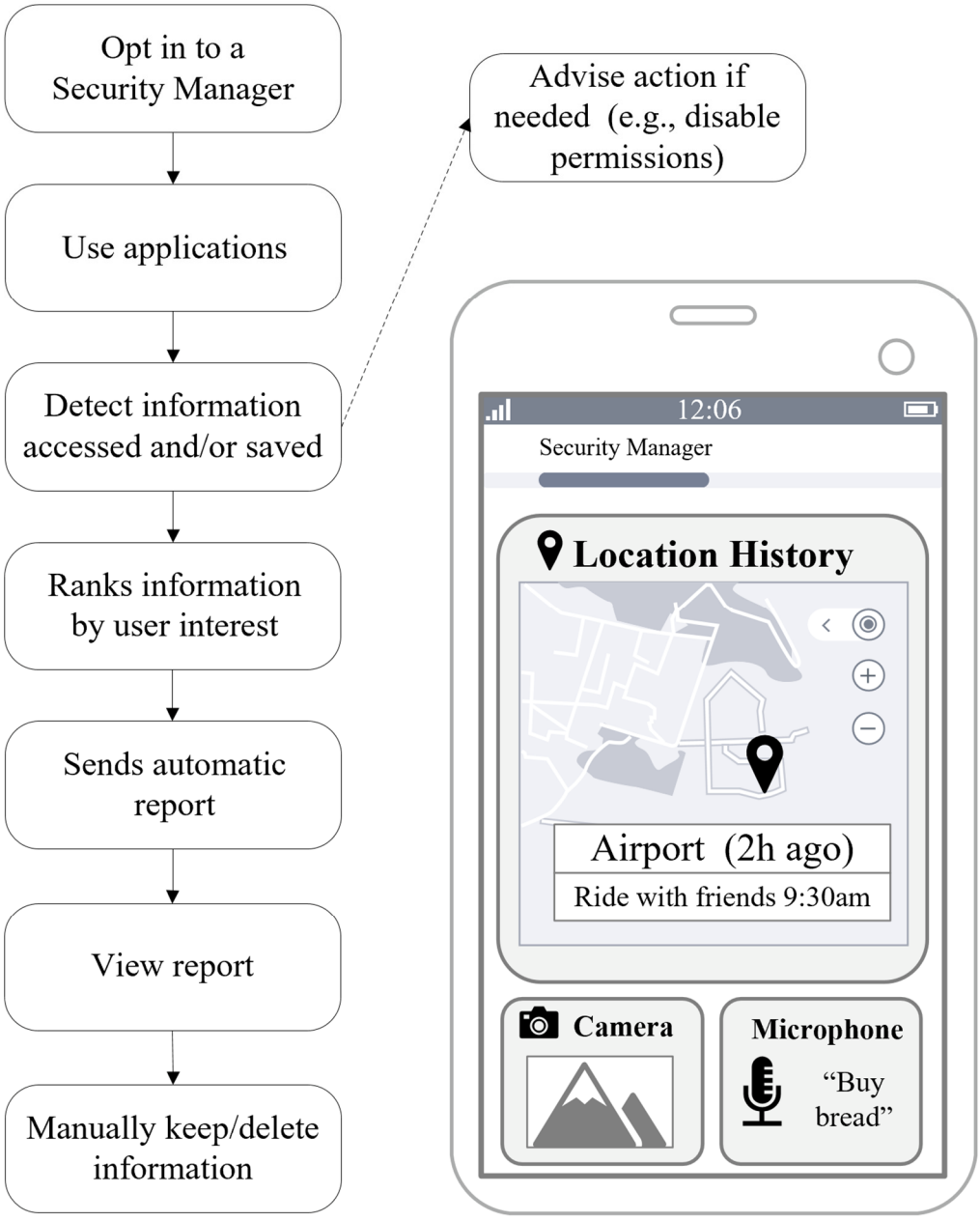


**Figure 1**

To monitor the information being collected and stored by applications, a user may opt in to a Privacy Manager as illustrated in Figure 1. The Privacy Manager may detect information collected by physical sensors, information stored on the computing device (e.g., as user data on the CRM), and information saved off the device (e.g., in the "cloud").

The operation of assessing privacy risks may require the Privacy Manager to rank information collected by physical sensors in terms of user-perceived importance (e.g., sensitivity). For example, information from a camera or microphone may rank high in terms of risk to the user, while inertial movement information may rank low. The Privacy Manager may also assess the risk level and determine if an action is advisable for the user. In an example, a shopping application may require location information from sensors to determine nearby stores. However, if the shopping application collects information from sensors that is not perceived to be relevant to the operations (e.g., collecting microphone data of personal conversations, accessing photo galleries), the Privacy Manager may flag the content and recommend an action for the user (e.g., disable permissions to physical sensors for that shopping application).

The Privacy Manager may periodically generate automatic risk reports and notify the user, for example, on the home screen of the computing device (e.g., a notification on the home screen that reads "Your new Privacy Report is available. Everything is secure."). The user may click on a notification to access a detailed privacy report of information recently collected by applications. The Privacy Manager may rank information collected by applications (e.g., from top to bottom) on the user interface page in terms of perceived risk to the user. For example, information collected about the location of the user may be located near the top of the user interface page with additional details collected by the application. In another example, a user may have taken a photograph of a meal and shared it with friends using a social media application on the computing device. The

photo, along with relevant details (e.g., date taken), may be identified on the user interface page of the Privacy Manager along with additional details collected by the social media application (e.g., date taken) to provide the user with a transparent technique to monitor the sharing of their personal information.

**References:**

[1] Patent Publication: US20110047594A1. System and Method for Mobile Communication Device Application Advisement. Priority Date: October 21, 2008.

[2] Patent Publication: US20170206351A1. Mobile Device Security Monitoring and Notification. Priority Date: July 22, 2014.

[3] Patent Publication: US20150381825A1. Mobile Application Usage Monitor. Priority Date: June 27, 2014.