Quickly Monitor and Control All Physical Sensors

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
N/A, "Quickly Monitor and Control All Physical Sensors", Technical Disclosure Commons, (November 24, 2020)
https://www.tdcommons.org/dpubs_series/3803

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
Quickly Monitor and Control All Physical Sensors

Abstract:

This publication describes techniques to turn on and off physical sensors of a computing device to protect user privacy. Users may be afforded a quick and easy way to turn on and off all physical sensors using a Privacy Manager that can be activated, for example, with a “sensor mute” icon located on the user interface or a physical switch located on the computing device. Users may monitor and/or customize the activity (e.g., on/off settings) of each sensor in a centralized control setting on the computing device. The Privacy Manager may identify each physical sensor of the computing device and list them in a centralized control setting with a short description of their use (e.g., an “activity sensor” is identified and used for “health screening”). The user may be able to customize their privacy settings by individually turning sensors on and off to meet their needs.

Keywords:

Privacy mode, secure, confidential, device sensors, detectors, microphone, camera, accelerometers, activity sensors, physical sensors, centralized control, control settings, application permissions, disable, disable sensors

Background:

There is a growing concern among users to protect their privacy. Some users spend significant portions of their day either using a computing device (e.g., a smartphone) or being near a computing device that can collect data about the user (e.g., through physical sensors). These
sensors can include, for example, cameras, compasses, microphones, proximity sensors, gyroscopes, accelerometers, barometers, ambient light sensors, and radar sensors. Even if the user is not actively using their computing device, these sensors may still be collecting data of, for example, the location of the user, sounds detected by the computing device (e.g., voices), and so forth.

The information obtained by computing device sensors can be considered confidential, causing some users to become concerned about their privacy. For example, users may be concerned about whether or not the microphone on their computing device is actively collecting data without their knowledge. Even though a user may opt in to an application on their computing device that requires contextual information from these sensors, it is not always obvious, for example, which sensors are being used, what data is being collected, and when the sensors are actively collecting data.

**Description:**

This publication describes techniques for quickly turning on and off computing device sensors and for monitoring and controlling the activity of each sensor in a centralized setting.

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., cameras, compasses, microphones, proximity sensors, gyroscopes, accelerometers, barometers, ambient light sensors, and radar sensors), a computer-readable medium (CRM), and an input/output device (e.g., a display, a speaker, a microphone). The CRM may include any suitable memory or storage.
device, for example, 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) that 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 turn the physical sensors on and off and provide the user with a central setting to monitor and control the activity of each sensor.

As illustrated in Figure 1, the Privacy Manager may allow users to quickly turn all sensors on or off at the same time, for example, with a “Sensor Mute” switch/toggle on the computing device. While the sensor switch illustrated in Figure 1 is a feature of the computing device software, this could also be a physical switch, for example.

The operation of quickly turning sensors on and off may require the Privacy Manager to communicate the sensor settings from the user input to each physical sensor. In an example, if the user switches the Sensor Mute on (e.g., with the intent of turning all sensors off), the Privacy Manager will detect the user input and turn the sensors off. However, if the user would like to use an application installed on the computing device that requires contextual information from physical sensors, then the user may need to turn the Sensor Mute off to allow the collection of contextual data needed to perform the application tasks (e.g., a location sensor may need to be turned on when using a map/directions application).
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., information about the social network of a user, social actions, social activities, profession, preferences of the user, a current location of the user) 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.

The Privacy Manager may allow a user to clearly monitor the computing device sensors and customize the activity of each sensor individually. The Privacy Manager may further provide a centralized control setting that identifies the physical sensors of the computing device, for example, to provide transparency on data collection to the user. The operation of identifying
sensors may require the Privacy Manager to label each sensor (as illustrated in Figure 2) with a name and short description of how the sensor is used to collect data. In an example, if the computing device of the user has an Activity sensor(s), the Privacy Manager may identify the physical sensor and label it as “Activity sensors” in a central control setting and best describe its use as “health screening.” While the purpose of each sensor may not be limited to the function identified in this brief description, a description may help users better understand the purpose of sensors, especially if it is not common knowledge. In an example, computing devices may have a gyroscope sensor to measure the physical orientation of the computing device (e.g., for automatic rotation of the orientation of user interface content as the computing device is rotated). A user may not be familiar with a gyroscope sensor and therefore not understand how it may be used on their computing device. If a user does not understand the function of a sensor, it may be difficult to decide whether or not it should remain active on the computing device.

Although the Privacy Manager may afford the user with an option to turn all sensors on and off easily, a user may desire to customize the activity of each sensor. The operation of turning individual sensors on and off may require the user to access a list of physical sensors on a centralized control setting provided by the Privacy Manager. The user may then select individual sensors to turn on and off. In an example, a user may want to turn their microphone off if they are having a private conversation but keep their camera on so they can use face detection to authenticate access to the computing device with ease. In this example, the user would need to custom turn off the microphone sensor and turn on the camera sensor using the Privacy Manager centralized control setting.
Figure 2

References:


