July 2023

Selective Delivery of Private Information on Device Lock Screen in Trusted Contexts

Sneha Ashok

Selective Delivery of Private Information on Device Lock Screen in Trusted Contexts

ABSTRACT

To avoid inadvertently revealing private information, delivery of query responses and notifications is restricted when a device is in a locked state, based on user configuration. In many contexts, e.g., when using the device in a hands-free mode while engaged in activities such as cooking or driving, the user can benefit from receiving such information without having to unlock the device. This disclosure describes techniques that permit users to receive results on the device lock screen for queries made to a virtual assistant and for notifications without needing to unlock the device first. The techniques provide flexible display of query responses or notifications with private content on the lock screen of a locked device. In addition to always-on suppression or display of such content, the techniques also enable selective display on the lock screen when in trusted contexts but not otherwise.

KEYWORDS

- Locked device
- Lock screen
- Private information
- Sensitive information
- Virtual assistant
- Voice match
- Trusted context
- Voice query
- Query results

BACKGROUND

The use of a virtual assistant via a smartphone or other device is commonplace, including when the device is locked. Based on the configuration of the virtual assistant, in some cases, when a user query is received by a device that is in the locked state, the user is requested to unlock the device to receive the responses to the query. For example, a user may configure the virtual assistant to only provide responses to queries that require use of certain user data (e.g., location, work address, etc.) when the device is unlocked. In such a case, if the user provides a query to a virtual assistant on a locked device such as "what time will I reach the office?" that requires the use of user data, the user is required to unlock the device to receive the answer.

The requirement to unlock the device prior to the provision of query results ensures that the person issuing the query is indeed an authorized user of the device. Such authentication ensures compliance with the virtual assistant configuration and prevents inadvertent disclosure of information to unauthorized parties. Depending on the configuration, the user may have to unlock the device even if a voice match technique is used to authenticate the user based on a spoken query.

In addition to query results, a user may also receive notifications with private information while the device is locked. On many devices, users are able to choose whether such notifications are shown on the lock screen of a locked device. However, such control applies globally to all notifications in all contexts, without the user being able to choose based on specific contexts and/or type/content of notifications.

DESCRIPTION

This disclosure describes techniques that permit users to receive results on the device lock screen for queries made to a virtual assistant without needing to unlock the device first. The

techniques provide flexible display of query responses or notifications with private content on the lock screen of a locked device. In addition to always-on suppression or display of such content, the techniques also enable selective display on the lock screen in a trusted context but not otherwise.

Users can choose to receive results without unlocking the device even in cases where the results may contain private and/or sensitive information. In order to receive such results in a secure manner that avoids unauthorized access, delivery of such results to the lock screen of a locked device is restricted to situations in which the user is a trusted context, such as at home, in their car, etc. In such contexts, the query results are displayed after authenticating the user with a voice match technique (matching voice print with a stored voice print for the user), as configured by the user.

Determination of whether the user is in a trusted context can be made based on user-permitted data obtained from various device sensors, such as network, Bluetooth, location (e.g., whether the device is within a geofence), presence (e.g., via a smart display), etc. For example, the user can be determined to be in their car based on the Bluetooth connection between the device and the media console of the car. The user can choose to specify which contexts are to be deemed as trusted for delivery of query results or notifications to the lock screen while the device is locked. In all other contexts, the user must unlock the device prior to receiving query results.

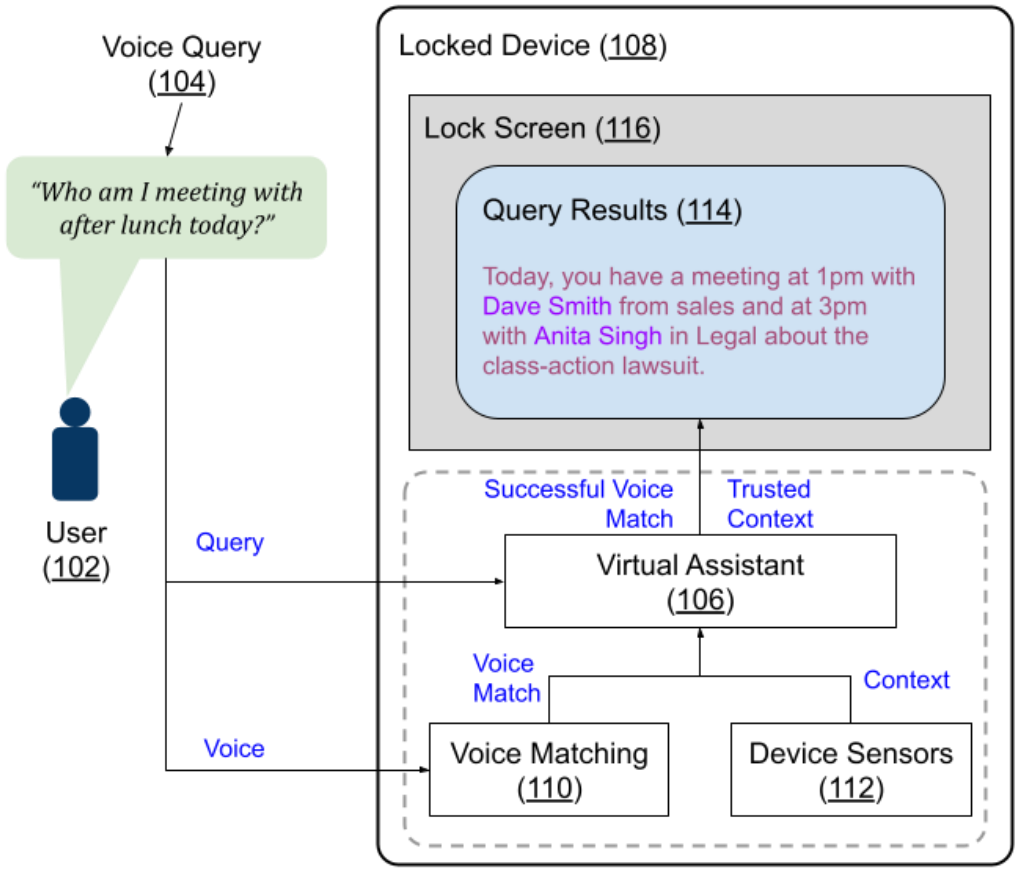

Fig. 1: Delivering query results to the lock screen of a locked device in trusted contexts

Fig. 1 shows an example operational implementation of the techniques described in this disclosure. A user (102), who has chosen to receive query results on the lock screen in trusted contexts, issues a voice query (104) to a voice-based virtual assistant (106) provided via a device (108). The user issues the query while the device is in the locked state. The spoken query is utilized to perform a voice match (110) with the user's known voice print. The user's current context is determined based on data obtained from the device sensors (112).

If the voice authentication is successful and the user is in a trusted context, query results (114) are provided on the device lock screen (116), regardless of whether the results contain private information. As shown in Fig. 1 shows, the results shown on the lock screen include private information about the user's post-lunch meetings, including meeting topics and attendees.

If the voice authentication fails and/or when the user is not in a trusted context, the user is asked to unlock the device in order to receive the query results.

Apart from serving results for voice queries to a virtual assistant, the techniques described herein can also control the delivery of other types of information to the lock screen of a locked device, regardless of sensitivity. For instance, the user can enable delivery of private or sensitive information such as reminders, notifications from applications, results of scheduled and automated actions, etc. on the lock screen of a locked device when the device is in a trusted context. Such notifications can include, e.g., unread text or email messages, information regarding the user's commute, upcoming calendar events, reminders from a to-do list, etc. As appropriate, based on the context and user preferences, such information can be delivered on the display screen (of the locked device or a paired device) and/or as audio.

The described techniques can be implemented to support any virtual assistant and any device. Users can be provided a preference setting to choose whether they wish to receive private information on locked devices in trusted contexts. Implementation of the techniques reduces the burden of having to unlock a device to receive information. The ability to avoid switching out of hands-free mode or paired mode to receive information on a locked device in trusted contexts can enhance convenience and safety when engaged in other actions, such as driving.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's voice queries, calendar and schedule, notifications, social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used,

so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes techniques that permit users to receive query results and notifications that include private information on the device lock screen for queries made to a virtual assistant and for notifications without needing to unlock the device first. The techniques provide flexible display of query responses or notifications with private content on the lock screen of a locked device. In addition to always-on suppression or display of such content, the techniques also enable selective display on the lock screen when in trusted contexts but not otherwise.

REFERENCES

1. Sharifi, Matthew, and Jakob Foerster. "Selective obfuscation of notifications." U.S. Patent 10,346,223, issued July 9, 2019.