22 Jul 2024

Context-Aware Dynamic Content Modification for Enhanced Privacy

Ramprasad Sedouram

Bindiya Mutum

Karthik Srinivas

Harshita Passi

Gulmohar Khan

See next page for additional authors

Inventor(s)
Ramprasad Sedouram, Bindiya Mutum, Karthik Srinivas, Harshita Passi, Gulmohar Khan, and Ajay Prasad

Context-Aware Dynamic Content Modification for Enhanced Privacy

ABSTRACT

In many contexts, a user needs to display on-screen content on their personal devices to others. In such situations, there is a concern regarding the potential exposure of personal information when others view the device screen. This disclosure describes techniques to automatically modify displayed content on a user device based on the context to provide a privacy-secure user experience that is seamless and enables users to display their device screens to third-parties. With user permission, data from various device sensors are analyzed, e.g., using on-device machine learning models, to automatically detect situations in which a device screen may be viewable by a third-party. Alternatively, a user can activate privacy mode by simply turning the phone around so that it faces away from the user which can be detected based on data from device sensors, or by invoking a privacy-safe mode via the device user interface. Once it is determined that privacy-safe mode is to be invoked, on-device machine learning models are utilized with user permission to analyze the displayed content to detect and mask personal information. During the time the device screen is being viewed by a third-party, other device functionality is disabled to ensure user privacy.

KEYWORDS

- User interface modification
- Private content
- Privacy screen
- Phone orientation
- Digital payment
- Screen sharing
- On-device machine learning
- Image masking
- Content masking
- Privacy preservation
- Payment confirmation
- Contextual privacy

BACKGROUND

Personal devices such as smartphones have become indispensable tools for various daily tasks such as navigation, communication, digital payments, etc. However, as user reliance on these devices increases, users often find themselves in situations where they need to display their device screen to others for specific purposes. For example, such purposes can include identity verification (e.g., showing a digital ID or a scanned version of a physical ID on a smartphone screen), transaction confirmation (e.g., showing payment confirmation from a digital payment app to a payment recipient), ticket presentation, etc. While these interactions are necessary in various social and professional contexts, there is a concern regarding the potential exposure of personal information stored on these devices when others view the device screen.

The challenge lies in the fact that many such interactions require users to show their device screens that display specific information. However, while viewing the screen, others may be able to view data from other apps of the user device. For example, while displaying a ticket or a boarding pass, a notification may be inadvertently viewable by the viewing party. Information that may be viewable by another party can include unmasked account numbers, identity numbers, passwords, personal photographs/videos, messages, etc. Manually hiding such information or updating device settings each time there is a need to show their device to another person is a time-consuming and cumbersome process and may not address all scenarios.

Physical privacy filters (privacy screens) ensure that a device screen is visible only from within a range of angles. Some software applications allow users to selectively hide or blur specific areas of the device screen, ensuring that sensitive information remains concealed. Some operating systems and device manufacturers have also incorporated built-in privacy features. For example, a screen pinning feature on some smartphones enables users to temporarily lock the

screen on a specific app, preventing others from accessing other parts of the device. However, such features do not override the device functionality. Some devices include secure folders or apps that provide an encrypted space where private information is stored. Such folders can only be accessed only with a password or biometric authentication. However, none of these solutions address the privacy challenge adequately and are also difficult to incorporate into daily use patterns.

In addition to hiding private information, there are also other factors that may help provide a better viewing experience for a third-party. For example, currently there is no way available to tailor the device display screen for a third-party, e.g., adjusting for readability under different lighting conditions, accounting for vision problems (e.g., color-blindness, inability to read text below a certain size, etc.), accounting for language understanding capability (e.g., when the third-party is unable to read the language content is displayed in), situational challenges with holding/displaying the device, etc.

DESCRIPTION

This disclosure describes techniques to automatically modify displayed content on a user device based on context to provide a privacy-secure user experience that is seamless and enables users to display their device screens to third-parties without having to perform cumbersome manual actions. Briefly, with user permission, data from various device sensors are analyzed, e.g., using on-device machine learning models to automatically detect situations in which a device screen may be viewable by a third-party. Alternatively, a user can activate privacy mode by simply turning the phone around (so that it faces away from the user) which can be detected based on data from device sensors such as accelerometer, gyroscope, face sensor, etc.; by

performing a shake action (or other gesture), or by invoking a privacy-safe mode via the device user interface.

Once it is determined that privacy-safe mode is to be invoked, on-device machine learning models are utilized with user permission to analyze the displayed content to detect and mask personal information. The user interface can also be modified to improve readability based on the context of the interaction. For example, if the third-party viewing the screen is detected to be at a distance (e.g., based on data from an infra-red sensor), the displayed font size can be increased; for different light conditions, screen brightness/ contrast can be adjusted; etc. During the time the device screen is being viewed by a third-party, other device functionality is disabled to ensure user privacy. The techniques are explained in detail below with reference to a digital payment application.

Example: protecting user privacy during digital payment

Consider a situation where a user has successfully completed a payment to a merchant using a digital payment application on their smartphone. The user wants to provide transaction confirmation to the merchant and for this purpose, needs to show their smartphone to the merchant for the merchant to view the transaction confirmation page. This context is recognized as an event where the device is to be shown to someone other than the device owner. As the user turns the smartphone towards the merchant, data from various sensors (e.g., accelerometer, gyroscope, face recognition, etc.) are accessed and analyzed with user permission to recognize the physical "turn" event. Also, the context that the payment application is active, and a payment confirmation is being displayed is determined from the currently active app.

An on-device machine learning model, trained to detect and mask personal data of various types, is utilized to analyze the displayed content, detect personal information, and to

modify the content to mask the personal information. For example, pixels in the UI that correspond to masked content may be modified (e.g., in-painted to match neighboring, non-private pixels; updated to display placeholders; etc.) or alternative user interface may be generated that includes the same content but excludes the personal data. For example, personal information that is detected and masked can include credit card number, digital payment identifier, government identifier, address, financial information such as account balance, etc. The user is provided with options to select the information that is to be shown or hidden in various contexts. When the device is ready for display content modification for user privacy, feedback can be provided to the user, e.g., unique haptic feedback that indicates that the privacy mode has been activated.

Additional information like ambient sunlight, brightness settings, the distance of the reader from the device's front (using IR sensors or other similar technology), the device location, ambient noise, etc. can be incorporated to alter content output based on user preferences. Settings such brightness/contrast, font size, audio volume level, etc. may be adjusted based on such information. While the device is turned towards a third-party, other functionality of the device is disabled to prevent inadvertent display of user information. When the device is turned towards the user again (as detected using sensors), such functionality is reenabled.

The entire process of detection of third-party viewing, detecting personal information, and masking the personal information is performed locally on the device. The process can also be initiated upon user-demand, e.g., upon detecting a shake gesture, a prolonged touch gesture, etc. or selection of a UI option by the user. The privacy-safe mode can be turned off automatically when the user is back in the field of view of the device camera or manually based on authentication.

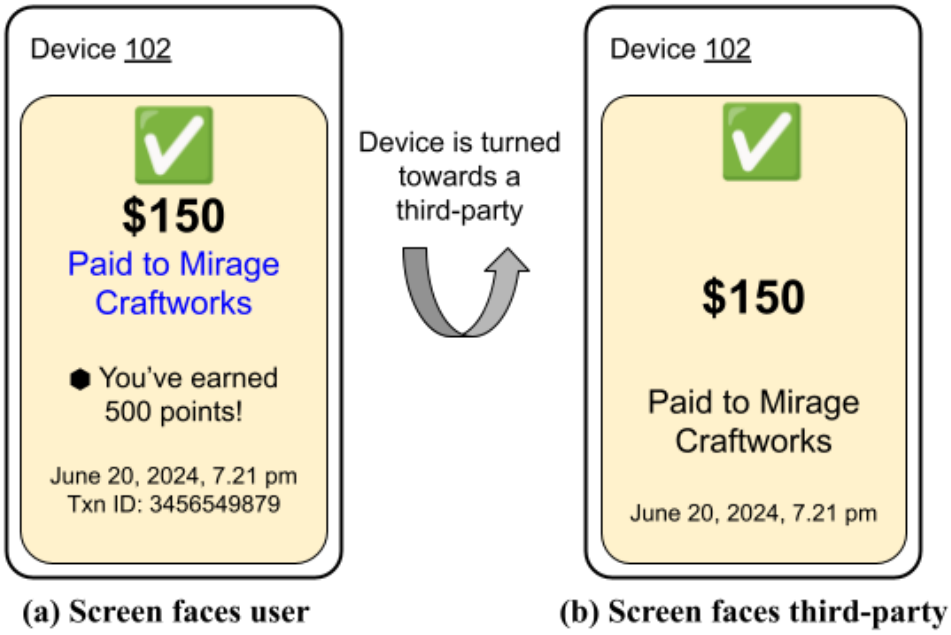

Fig. 1: Dynamic content modification for private and secure payment confirmation display: (a) device faces the user - content is displayed without masking personal data; (b) device faces a third-party - private information is masked

Fig.1 illustrates an example of dynamic modification of displayed content on a device (102) to provide a privacy-secure user experience. In the example of Fig. 1, the user has made a payment using a digital payment application. Upon completion of the payment, the UI of Fig. 1(a) is displayed on screen, providing confirmation of the payment and including additional information such as points earned and transaction ID. When it is detected that the user has turned the device towards a third-party, e.g., a merchant that the payment was made to, the displayed content is modified to hide private information, as shown in Fig. 1(b). The device seamlessly transitions from displaying the full payment confirmation with personal data to a privacy-safe version of the same information, thereby ensuring user privacy without compromising the overall user experience or the ability to share necessary information with others.

In another example, a point-of-sale (PoS) device that is to be turned towards a customer, e.g., for them to enter information such as payment authentication, the UI may be modified to hide merchant's private information and to disable other functionality.

While the foregoing description refers to a digital payment app on a smartphone, the described techniques can be used to enhance privacy for any app on any device. The techniques can be utilized in virtual reality or mixed reality. For example, when a user views UI objects superimposed on the real world or as part of a virtual world and attempts to flip the objects to show them to other participants in the same world, the flipped objects are modified to hide personal information.

In another example, foldables or other devices that have screens on multiple sides can display different versions of the UI on the different screens. For example, a private version can be shown on the screen facing the primary user of the device, while other screens can display a modified UI. In another example, augmented reality objects (e.g., a payment confirmation object) that include privacy content can be modified using the techniques described herein before the objects are shared with a merchant for the merchant to view via their AR glasses.

Contextual UI modification provides a seamless experience and provides user convenience while preserving user privacy. By performing device state detection, private information detection, and UI modification on-device, the techniques make privacy-preserving viewing of user interfaces possible without the user having to send data to a remote computer, and even when the user device is offline. The described techniques can be implemented in individual applications (e.g., a digital payment application) and/or as part of a device operating system.

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 device orientation, content displayed on a device screen, a user's context, 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 to automatically modify displayed content on a user device based on the context to provide a privacy-secure user experience that is seamless and enables users to display their device screens to third-parties. With user permission, data from various device sensors are analyzed, e.g., using on-device machine learning models, to automatically detect situations in which a device screen may be viewable by a third-party. Alternatively, a user can activate privacy mode by simply turning the phone around so that it faces away from the user which can be detected based on data from device sensors, or by invoking a privacy-safe mode via the device user interface. Once it is determined that privacy-safe mode is to be invoked, on-device machine learning models are utilized with user permission to analyze the displayed content to detect and mask personal information. During the time the

device screen is being viewed by a third-party, other device functionality is disabled to ensure user privacy.

REFERENCES

1. “Hide sensitive account data with discreet mode - N2 " available online at https://n26.com/en-eu/blog/discreet-mode accessed Jul 5, 2024.
2. “Privacy Virtual Cards” available online at https://privacy.com/ accessed Jul 5, 2024.