December 14, 2018

Securing private images on user devices

Linden Evans

Laura Paragano

Securing private images on user devices

ABSTRACT

This disclosure describes techniques to secure and remove private images (e.g., photos) from display on user devices. With user permission, a device examines stored user images for private content and relocates detected private images to a locked album on the device. The private album can include user-adjustable settings to control the organization and distribution of private images. Such features enable the device to automatically seclude private images, thus removing such images from potential undesirable discovery by other users that may use the device or other devices that access a collection of images on the device.

KEYWORDS

- photo library
- locked album
- private photos
- image access
- backup
- restricted access

BACKGROUND

Personal devices such as smartphones are able to capture and store thousands of personal images such as photos as well as videos. Online photo-sharing services allow a user and other permitted users to easily access and view a collection of the user's images and videos. However, there may be certain images that users may prefer to not be visible to other users, referred to herein as private images. Such images can include, e.g., images that capture private or personal moments and scenes, images that include personal information such as financial and

identification documents, information related to the user's health, etc. Current photo libraries typically do not exclude such images in the user's image collection when the collection is displayed to other users. This is undesirable when other persons access and view the user's collection of images.

For example, if the user gives the user's device to another person to view images in the collection on the device, private images could be viewed by the person, with no option at that time for the user to restrict access to the private images. In another example, a different user's device may access the image collection over a network, e.g., on a photo-sharing service or by remotely connecting to the user's device. Such access could result in unintentional sharing or viewing of private images. In addition, images in the user's collection may often be automatically backed up, e.g., to storage in the cloud. While appropriate for most of the user's images, this increases the risk that private images in the collection may be obtained or accessed by other persons.

Some devices may provide options to manually move private images to other storage locations or specify the access level of such images,. However, this is an onerous task when the user has many images in the collection. Other techniques simply blur or obfuscate a private image in the image gallery view of a device's photos management application. However, it is still evident to a user that there is an image present that includes content that was not desired to be viewed.

DESCRIPTION

This disclosure describes techniques that automatically detect private images (e.g., photos, videos) in a user's image collection and automatically secure and safeguard such detected images from access by other persons. Described techniques provide various settings

for securing the private images that can be adjusted by the user, allowing customization to the process.

The techniques described herein are implemented upon specific user permission to access a user's images and to detect image content. Only images, videos, and image/video metadata for which the user grants permission are examined and processed.

These techniques can include automatically determining whether an image is a private image, securing the identified private image in a private album, and adjusting settings for such albums or images.

Identification of private images

With user permission, the present techniques cause a user device to examine the images in a user's image collection and automatically identify images that likely qualify as private images to the user. For example, the techniques can utilize trained machine learning models to identify and tag potentially private content in images. Private content can include, for example, depictions of personal information (e.g., identification documents such as passports and driver's licenses, financial statements or other information, medical information, etc.), explicit content (e.g., nude or semi-nude persons, pornography), profanities, etc. and other content that is unsuitable for viewing by other persons. For example, the model may be trained with training data (obtained or created specifically for this purpose) images and videos that depict various types of private information. Such a model can then recognize such information in new images and videos. In some cases, image metadata can be used in the training process.

The described machine learning models can be implemented on a user device, e.g., a mobile device or other device. If user permission is obtained, the models can be fully or partially implemented on a server or other remote device in communication with the user

device. In some cases, heuristics and rules can be used instead of or in addition to machine learning models.

Furthermore, images detected as having private content can be clustered into different classifications according to different types of private content (e.g., identification information, financial information, explicit content, etc.), such that each different type of private information is represented by an associated classification or identification. In some examples, a model can be trained using both positive and negative examples of different classifications or types of private content.

If an image is detected to include private content, the device updates the metadata tags of the image accordingly. For example, the metadata is updated to include a "private" indicator for the image.

In some examples, upon capture of a new image, the user device checks the new image for private content and tags detected private images. Furthermore, previously-captured stored images not previously examined for private status can be processed similarly.

Upon detection of a potentially private image, the device prompts the user to confirm that a selected image should be marked and stored as a private image. For example, if the confidence that the image includes private content is above a high threshold, the image is automatically tagged as private, and if the confidence is below the high threshold but above a second threshold, such a prompt is provided.

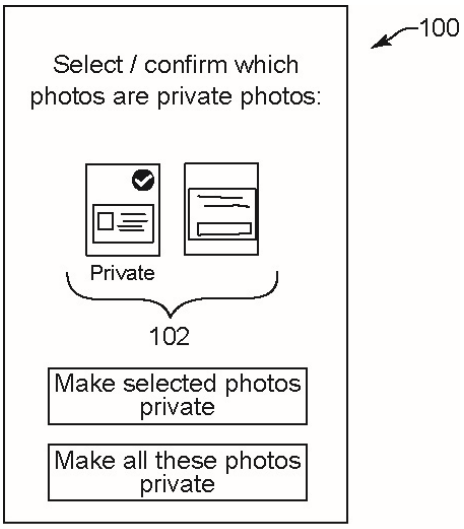

Fig. 1

Fig. 1 shows an example of such a prompt in a user interface (100) displayed on a device. The interface displays new images (102) that have been detected as potentially private images, but the confidence level is below the high threshold. The user can indicate which of the displayed images are to be made private images.

The device can provide user-adjustable preferences or settings that allow the user to specify particular content or particular types of content, such that images depicting such content is always presented to the user for confirmation before tagging as private images.

Securing identified private images

After private images (including videos) of the user's collection have been identified, the private images are secured and separated from the other images and videos of the user's image collection. For example, private images are automatically relocated into a separate locked album, folder, or other container. For example, the private images can be relocated to a locked album accessible by a photo management application on the user device.

Advantages of relocating private images to a different album than a main gallery album are that the content of the private images is protected from access and the existence of such private images is unknown to other people viewing the main gallery. The separate album also allows a user to manage private images, e.g., review, edit, delete, etc. the images, in a single location instead of having to scroll through the full collection of images to find private images.

No user except the owner of the device is authorized to access the private album. The images within the album as well as the metadata of these images are protected from access by other users. For example, access to the private album is protected with one or more authentication techniques, e.g., the user can designate a password or PIN, can require use of a fingerprint sensor, can require face recognition, can require multiple-step authentication, etc. to allow access to the private album. Thus, if a different person were navigating through the user's photo management application, that person wouldn't be able to access the private album and the private images within it.

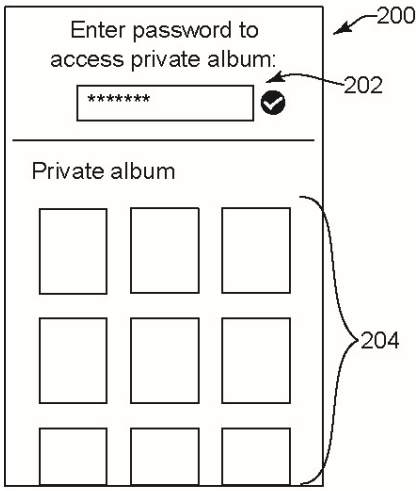

Fig. 2

Fig. 2 shows an example user interface (200) displayed on a user device, where a user has been prompted at an input field (202) to input a password to access the images of a private

album. In this example, the user has input a valid password, causing private images (204) of the private album to be displayed, e.g., in a scrolling format as shown.

In further examples, multiple private albums can be created and different types of private images can be located in respective private albums, allowing the user to organize and quickly access particular types of private images. In some cases, different authentication methods and/or different passwords or PINs can be used for different albums. For example, a particular type of private content can be considered the most sensitive by the user, and can require 2-step authentication prior to access, while other types of private content are designated to require only one step authentication.

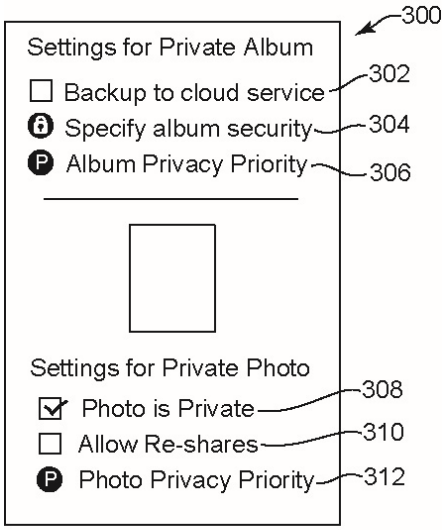

Fig. 3

Adjustable settings for private album and private images

The user is provided a user interface that enables adjustment of various settings for a private album and for the private images in the private album. Fig. 3 shows one example of a user interface (300) displayed on a user device, e.g., as part of a photo management application. The interface provides adjustable settings for a private album or for a particular private image

in that album. For example, the private image may have been selected by the user, e.g., using the user interface of Fig. 2.

A backup album setting (302) for the private album is specific to the private album, allowing the user to specify whether or not the private album is to be backed up, e.g., to a server in the cloud, a backup device, etc. This provides the user with control over the digital storage locations where private images are duplicated and stored. For example, if a user consents to having the private images backed up, the photo management application syncs the private images, e.g., to cloud-based storage. The user can turn the backup function off such that the images are only stored locally on the user device to minimize the risk of other users being able to access the private images.

Another adjustable setting for the private album can include an album security setting, e.g., setting 304 in Fig. 3. For example, the user can select this setting to specify a security level for the album (e.g., using options in additional user interfaces), such as the type(s) and security level of authentication methods to be used to access that album. Another adjustable setting for the album can include a privacy priority setting, e.g., setting 306 in Fig. 3, which can be selected to specify a priority level for the album (e.g., using options in additional user interfaces). If multiple private albums are created for a user, then each such album can be assigned its own priority level. Each private image can be assigned a priority level (see below) such that images having a particular priority level can be placed in a private album having the corresponding priority level.

Image-level adjustable settings are also provided for each private image stored in the private album. In the example of Fig. 3, a private image 308 has been selected by the user and is displayed in the interface for reference. A private setting (310) allows the user to specify or

adjust the private status of the image, e.g., change a privacy tag in the metadata of the image. For example, a private image can be changed to a non-private image or vice-versa. For example, in a case where the device incorrectly marks an image as private or vice-versa, the user is able to manually mark the image as private or non-private in the settings. In response, the metadata is changed, and the system automatically relocates the image into (or out of) the private album based on the new private status. Backup settings for that image are also adjusted based on the new private status, e.g., causing removal of any backup image from the cloud or causing the image to backed up to the cloud accordingly.

A re-shares setting (310) for an image allows or disallows re-shares of the private image by other users who have received the private image from the user. For example, if the user using a first device shares a private image with recipient user using a second device (having a compatible photo management app), the private metadata tag is recognized by the second device and the image is automatically sorted into the recipient's private album. Then, if the re-share setting of the private image allows it, this recipient user is provided the ability to send that image to other users. This setting allows a user to prevent, if desired, a shared private image from being distributed to additional users from a recipient device. In some examples, all private images can be located in a single private album of the recipient device, or the recipient device can provide a respective private album associated with each user from whom private images are received, such that private images received from multiple users are not grouped within a single private album of the recipient device.

In some examples, a recipient device that stores received private images checks for actions on the recipient device that are related to the private images. If, for example, the recipient user inputs a command to obtain a screen capture of another user’s private image, the

recipient device can ignore the command. In other examples, a screen capture is allowed, but the recipient device examines the content of the captured image, and if the content matches (e.g., is above a threshold similarity to) the content of a private image received from another user, the recipient device designates the captured image to be a private image (e.g., associated with the same user and having the same settings as the matched image).

Another adjustable setting for the image can include a privacy priority setting, e.g., setting 312 in Fig. 3, which can be selected to specify a priority level for the image (e.g., using options in additional user interfaces). For example, a user can designate particular private images to have a higher-priority private status, and other private images to have a lower-priority status, and/or assign additional priority levels to other private images. Furthermore, other features and settings can be based on such priority levels. For example, the user can specify to back up priority-2 private images to the cloud, and to not back up priority-1 (higher priority) private images. Furthermore, multiple private albums can be provided, each private album associated with a particular priority level and storing private images having that priority level.

Machine learning models that are used to implement the described techniques are trained and implemented only with user permission to access user data that serves as input to the models. Users are provided with options to indicate permission or denial of permission for access to various data, e.g., images, image metadata, video, and other content in the user's image library, contextual factors such as time, location, application in use, etc. In implementing the described techniques, use is made only of user-permitted data, and certain techniques (e.g., ML models) are not implemented, if users deny permission. Model training is performed based on generalized data that is not attributable to individual users, and/or

performed only locally on the user device with user data, e.g., using a federated learning approach.

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 activities, social network, or social actions, profession, a user's preferences, or a user's current location), and if a user device 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 enable automatic determination of images of a user's collection that are private images, e.g., images that depict content that may be private to the user. The device automatically places such private images in a private album that is separate from other images in the user's collection and secures the private images from access by other users. This allows private images to be secured in particular storage locations, and prevents inadvertent viewing of such images by other users. Further, a variety of settings are provided that allow the user to control organization of private images and distribution of private images to other devices.