March 01, 2019

Restricting access to files by application programs

Sandro Feuz

Thomas Deselaers

Restricting access to files by application programs

ABSTRACT

This disclosure describes techniques to enable users to restrict private data from display. Such private data can include images, videos, documents, and other files, by a user device. Private files can be manually or automatically designated, and the content of these files is hidden from user interfaces provided by application programs. Automatic designation is performed using user-permitted techniques for automatic analysis of files. Further, a variety of settings allow the user to control access to private data for display by designated application programs. Such features restrict another user that is viewing a device screen from viewing private data. Described techniques provide these features in ways that reduce the impact on usability, where authenticated access to private data is easily permitted via displayed prompts.

KEYWORDS

- restricted access
- file access
- file permission
- private files
- private photos
- photo library

BACKGROUND

Personal devices such as smartphones store files of various types. For example, devices store files such as images (e.g., photos and videos), documents, audio files, etc. There may be certain files that include content which users prefer to not be visible to other users, referred to herein as private files. Such files can include, e.g., images that depict private or personal

moments and scenes, images or documents that include personal information such as financial and identification documents, health information, etc.

Many application programs on a user device access a user's files on the device to provide various functions. For example, chat applications access and display user images to allow the user to select images to send to other chat participants. Social media apps access and display user images to allow the user to select images to post or share to other users. Email, service applications, etc., access and display user images to allow the user to send or post images, select an image to use for a background for a user interface or for a user account avatar, etc. Such applications often use a "preview" mode in which a collection of the user's images is displayed to allow the user to select one or more images to process by the application. Such a mode typically displays several images on a user's device, e.g., to allow the user to browse the images, and can include user images that include private data. Such data from private images (and other types of private files) can be seen by anyone that views the display screen of the device.

DESCRIPTION

This disclosure describes techniques that allow a user to designate files as private files and/or automatically detect and designate private files by the user device. Described techniques provide various settings to restrict access to private files by particular application programs such that access can be customized by the user.

The techniques described herein are implemented upon specific user permission to access a user's files and to detect private files. Only files and metadata for which the user grants permission are examined and processed. Users are provided with options to select files to grant permissions to and/or to disable the techniques entirely. For example, the user can

enable or disable techniques discussed herein for particular directories or other groups of files, particular users or devices, etc.

Designating Private Files

The files associated with a user (e.g., content files stored on a user device or stored on a server and accessed, e.g., via a user account on a network service) can include files having data that is considered private and/or which the user deems to be private and prefers that display of such data be restricted. Such files are designated as private files. Private files can include particular types or classes of data. For example, private data can include depictions of personal information such as identification documents such as passports and driver's licenses, salary and financial data (e.g., tax forms), medical data (e.g., relating to the user and/or to patients, if the user is a medical professional), media of a personal nature, etc. Private data can also include images depicting the user at a party, images depicting a user performing a hobby activity, etc. Identifying a file as a private file can be a user-specific preference.

Designation of files as private can be performed manually by the user and/or can be automatically performed by a device.

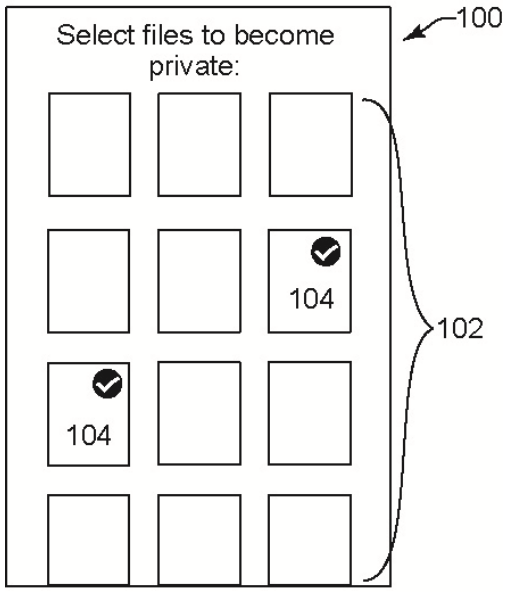

Fig 1: Selection of images to be made private

Fig. 1 shows an example of manual designation of files to be made private. In Fig. 1, a user interface (100) displays a list of files of the user. In this example, the files are displayed as thumbnail images (102 in a grid or list. To designate images as private, the user selects particular images via a standard input mechanism providing user input to the user interface. In this example, two files (104) have been selected by the user to be designated as private, e.g., by scrolling the list of images until the desired images are displayed in the user interface and tapping via a touchscreen (or otherwise selecting) the files.

With user permission, the present techniques also enable a device to automatically identify files that likely qualify as private files to the user. For example, the techniques can utilize trained machine learning models and applying machine learning classification to identify and tag potentially private data in files.

For example, the model is trained with training data (e.g., images, videos, documents, etc.) that include various types of private data, e.g., training data that is obtained or created

specifically for this purpose, and/or with user-specific training data. Such a model can then be applied to recognize private data in new files. In some cases, file metadata can be used in the training process. For example, the device starts with a common model that identifies private files, and is trained further based on private files identified or confirmed specifically by the user, if the user permits such personalization. Training data for the classifier can include or mimic various types of data such as health or medical data (e.g., analyzed using computer vision methods), financial data, image metadata such as time and location of capture, etc.

The machine learning models can be implemented on a user device, e.g., a mobile 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.

With user permission, images detected as having private content can be clustered into different classifications according to different types of private data (e.g., identification information, financial information, personal images, etc.), such that each type of private data is represented by an associated classification.

If a file is determined to include private data, e.g., based on manual user designation and/or automatic determination by the device, the device annotates the file accordingly. For example, the metadata of the file is updated to include a "private" indicator. Similar metadata or associated data of other types of private files (e.g., documents, audio files, etc.) can be similarly updated.

In some examples using automatic private data detection, upon receiving new files (e.g., capture of a new image or video), the user device checks the new file for private data and updates the metadata of detected private files. Previously-captured stored files not previously

examined for private data can be processed similarly, if permitted by the user. Upon detection of a potentially private file, the device prompts the user to confirm that a selected file is to be designated as a private file. With user permission for automatic classification, if the confidence that the file includes private data is above a high threshold, the file is automatically tagged as private, and if the confidence is below the high threshold but above a second threshold, such a prompt is provided. User-adjustable preferences or settings are provided that allow the user to specify particular types of data to require confirmation before tagging as private files.

Restricting Access to Private Files

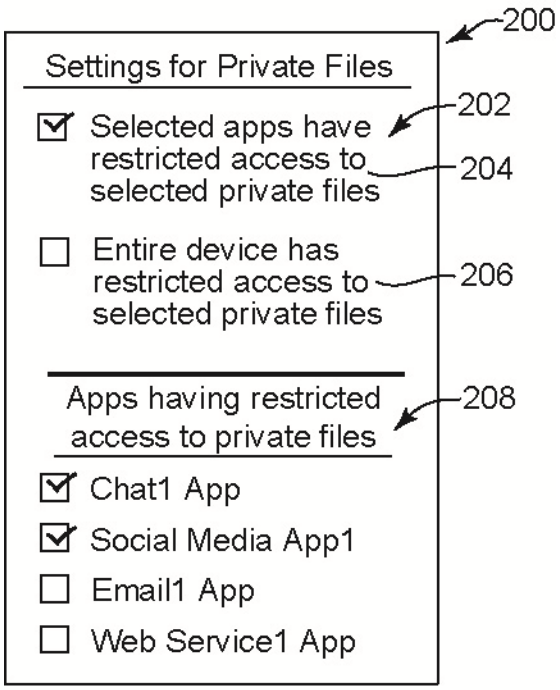

Fig. 2: Settings for private file access by application programs

Fig. 2 shows an example of a user interface (200) with settings that a user can specify relating to private file access by application programs. After manual or automatic designation of files as private as described above, the user can be presented with settings for the selected private files. In the settings (202), the user can select a first option (204) to designate selected

application programs to have restricted access to the selected private files, or a second option (206) to designate the entire device to have restricted access to the selected private files.

If the first option is selected by the user as shown, then the user can specify which application programs are restricted in accessing the selected private files. For example, in response to selection of the first option, additional app settings (208) can be displayed. These settings display application programs installed or available via the user device which have functions accessing the user's files, e.g., displaying images or data of other types of files for the user to browse and select, displaying files in a view or interface, etc. Input selections by the user in the app settings causes the selected application program(s) to have restricted access to the selected private images. If the second option is selected by the user, then all application programs on the device are restricted from accessing the selected private files.

The particular restrictions imposed on the restricted application programs can vary based on default or user-specified preferences. For example, the restriction can be exclusion of all access by the restricted application programs to the selected private files. In some examples, such exclusion prevents the selected private files from being visible to the application program, such that the selected private files are not accessible and are not displayed by the application program. In some cases, the exclusion allows the application program to detect the presence of private files (e.g., particular metadata of the files), and causes the program to display substitute images in place of the selected private images, e.g., see Fig. 3.

In other examples, the user can specify particular conditions under which the restricted application programs are allowed to access and/or display the selected private images. In an example, the conditions can include particular types of data in the selected private files (e.g., access is allowed for particular types of subjects depicted in a private image, e.g., landscape

features). In other examples, the conditions can include specified time periods and/or geographic locations of the device for which access and display is allowed. Particular conditions of restricted access can be defined as a device-wide setting associated with all application programs, or can be specified individually for each application program listed in the app settings.

The restrictions on access to private files can be implemented as a permission or through a device-wide setting, e.g., enforced by a device operating system. If an application program does not have the privilege to access a particular private file, then the device filters that file on every file system call from that application program. If an application program has full access to a private file, then the private file passes unfiltered to the application program.

The file system application programming interface (API) is configured to enable restricted access to private files. The API includes settings specifying how particular application programs are to treat private files when attempting to access the files. When an application program requests files for display, private files are removed from the returning list if the application program does not have access (metadata can be provided in some cases). When the application program reads the data of files, a read error is returned to the application program for files that are private, if the application program does not have access. When the application program writes files, nothing changes from the usual functionality.

In other examples, each application program can individually provide and implement the described access permissions to private files for that application program. This feature depends on the available functionality of the application program.

Displaying Private Files

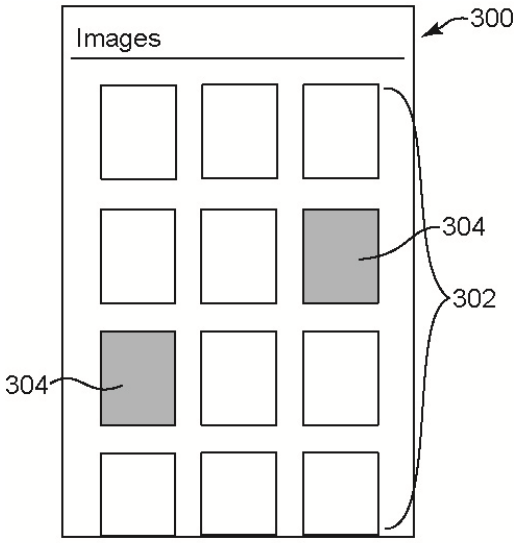

Fig. 3: Display of private images in an image grid

Fig. 3 shows an example user interface (300) in which a user's files are displayed. In this example, an image grid is displayed in the interface and includes thumbnail images (302) showing the content of associated full-sized images. The images are displayed in a particular order, e.g., based on capture date of the images, based on tags for subject matter in the images, etc. Additional images can be scrolled into view.

Private image representations (304) are also included in the grid in the user interface. The representations hide or obscure the content of the associated private images, thus preventing other users from seeing the image content. In this example, the private image representations are displayed as shaded rectangles. Various other representations can be displayed in other implementations, e.g., black images, blurred thumbnail images, etc. The private image representations are positioned within the grid of elements at locations where their associated private images would otherwise be displayed, e.g., based on capture date of the image or other ordering criteria. Private images may be displayed in other formats or orders.

In other examples, representations of private images are removed from the grid entirely, and are displayed upon request as indicated by user input to the device.

This display of the private image representations can have operating system level user interface support, such that when an application program does not have access to a private image, the representation is displayed in place of a standard image thumbnail of that image.

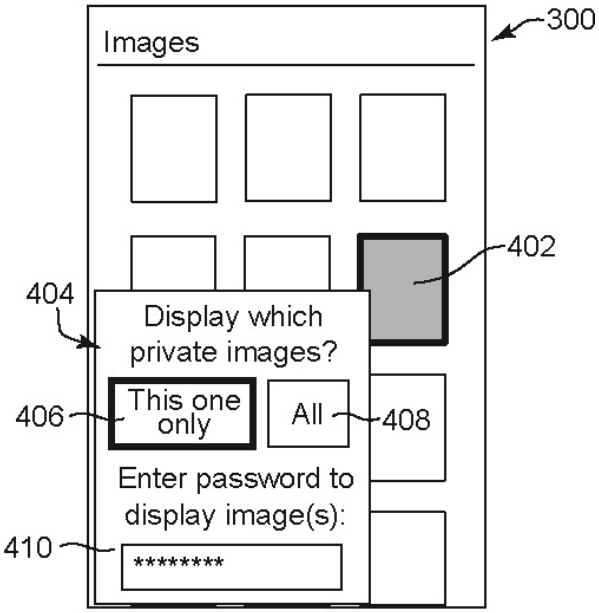

Fig. 4: Displayed prompt to access a private image

Fig. 4 shows the user interface (300) of Fig. 3 after the user has selected a private image representation (402). For example, the user has selected the representation using a touchscreen or other type of input device. In response to the selection, a prompt (404) is displayed. The prompt includes options to display private image thumbnails in the user interface. The user can select a first option (406) to display only the private image thumbnail associated with the selected representation, or can select a second option (408) to display all private image thumbnails in the user interface.

The prompt also includes an authentication input field (410) which receives user authentication to cause the selected private image thumbnail(s) to be displayed. In this example, the user enters a password or personal identification number (PIN) for authentication. In other examples, with user permission and upon configuration, the authentication can be a fingerprint via a fingerprint reader, face recognition via a camera, or a different form of authentication. In further examples, multiple-step authentication can be enforced. In other examples, the user can designate different authentication methods and/or different passwords / PINs for different types of file data. For example, a particular type of private data may require two-step authentication for access, while other types of private data require only one-step authentication.

Upon selection of an option and input of the authentication by the user, the selected private images are displayed. In some examples, the private images are displayed as thumbnail images in place of the representations in the grid, or the private images are displayed in a separate view or window.

Machine learning models that are used to implement some of the described techniques using user data 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 is provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein enable collection of user information (e.g., information about a user's 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 is 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 is treated so that no personally identifiable information can be determined for the user, or a user's geographic location is 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 has 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 users to restrict private data from display. Such private data can include images, videos, documents, and other files, by a user device. Private files can be manually or automatically designated, and the content of these files is hidden from user interfaces provided by application programs. Automatic designation is performed using user-permitted techniques for automatic analysis of files. Further, a variety of settings allow the user to control access to private data for display by designated application programs. Such features restrict another user that is viewing a device screen from viewing private data. Described techniques provide these features in ways that reduce the impact on usability, where authenticated access to private data is easily permitted via displayed prompts.