

CLAIMS

WHAT IS CLAIMED IS:

1. A mobile electronic device, comprising:
a camera;
an image signal processor;
one or more additional processors; and
a memory, storing program instructions, that when executed using the one or more additional processors, cause the one or more additional processors to:
implement an operating system (OS) for the mobile electronic device; and
forward data from the image signal processor and an appended identifier to
a secure storage repository, wherein the data and appended identifier
are forwarded to the secure storage repository using a secure
communication channel implemented at an OS layer below an
application layer such that the secure communication channel is not
accessible to applications executing on the mobile electronic device.
2. The mobile device of claim 1, further comprising:
a local storage,
wherein the program instructions, when executed using the one or more additional
processors, further cause the one or more additional processors to:
generate a copy of the data, wherein the data to which the identifier is appended
and forwarded to the secure storage repository is a first copy of the data;
and
provide, to the application layer, a second copy of the data, wherein the second
copy of the data is accessible to one or more of the applications executing
on the mobile device.
3. The mobile electronic device of claim 1, wherein the program instructions, when
executed using the one or more additional processors, further cause the one or more
additional processors to:

receive, via a user interface of the mobile electronic device, an indication that a given image captured by the camera of the mobile electronic device is authorized for public sharing; and
send an indication to the secure storage repository to provide, when presented with the identifier, a representation of the securely stored first copy of the data, wherein the first copy and the second copy of the data are usable to determine the second copy of the data is an authentic copy of original data from the image signal processor.

4. The mobile electronic device of claim 1, wherein the program instructions, when executed using the one or more additional processors, further cause the one or more additional processors to:

implement a secure enclave in the OS, at the OS layer below the application layer, wherein data in the secure enclave is not accessible to the applications executing on the mobile device;
receive, from the image signal processor, at the secure enclave, the data for an image captured by the camera; and
append, in the secure enclave, the identifier to the data,
wherein the secure communication channel connects the secure enclave to the secure storage repository at the OS layer.

5. The mobile electronic device of claim 4, wherein the program instructions, when executed using the one or more additional processors, further cause the one or more additional processors to:

append additional metadata to the data in the secure enclave, wherein the additional metadata comprises one or more of:
a date and/or time when the image was captured by the camera; or
a geographic location of the mobile electronic device when the image was captured by the camera.

6. The mobile electronic device of claim 4, wherein the program instructions, when executed using the one or more additional processors, further cause the one or more additional processors to:

implement a verification agent in the secure enclave, wherein the verification agent uses other sensor data captured in temporal proximity to the image by one or more other sensors of the mobile electronic device to verify that the data is of an authentic image.

7. The mobile electronic device of claim 6, wherein to determine the data is of an authentic image the program instructions, when executed using the one or more additional processors, cause the one or more additional processors to:

determine depth information for one or more objects in the image;
compare the determined depth information to depth data captured by the one or more other sensors of the mobile electronic device; and
refrain from submitting the image to the secure storage repository in response to determining the determined depth information deviates from the depth data by more than a threshold amount.

8. The mobile electronic device of claim 1, wherein the data from the image signal processor comprises one or more of:

an image;
a video; or
volumetric visual content.

9. A system comprising:

a secure storage repository; and

one or more computing devices storing program instructions, that when executed by the one or more computing devices, cause the one or more computing devices to:

receive from a mobile electronic device, via a secure communication channel, a copy of data captured by a camera of the mobile

electronic device, wherein the secure communication channel connects the one or more computing devices to the mobile electronic device at an OS layer below an application layer such that the secure communication channel is not accessible to applications executing on the mobile electronic device;
store the copy of the data captured by the camera of the mobile electronic device in the secure storage repository; and
provide, in response to an authentication request, a representation of the stored copy of the data captured by the camera.

10. The system of claim 9, further comprising:
an additional storage repository,
wherein the one or more computing devices store program instructions that, when executed by the one or more computing devices, cause the one or more computing devices to:
receive from the mobile device, or another source, an additional copy of the data captured by the camera of the mobile electronic device via a separate interface, separate from the secure communication channel;
store the additional copy of the data captured by the camera of the mobile electronic device in the additional storage,
wherein the additional copy of the data captured by the camera stored in the additional storage is editable; and
wherein the copy of the data captured by the camera stored in the secure storage repository is not editable.

11. The system of claim 9, wherein the program instructions, when executed by the one or more computing devices, cause the one or more computing devices to:
compare metadata included with the authentication request to metadata stored in the secure storage repository for the copy of the data captured by the camera of the mobile electronic device,

wherein said providing the representation of the stored copy of the data captured by the camera is performed in response to determining a match between one or more items of metadata included with the authentication request and one or more items of metadata stored in the secure storage repository for the copy of the data captured by the camera.

12. The system of claim 11, wherein the one or more items of matching metadata comprise one or more of:

an identifier appended to the data captured by the camera stored in the secure storage repository and an identifier provided with the authentication request; or

a date and/or time the data was captured that is stored in the secure storage repository and a date and/or time provided with the authentication request.

13. The system of claim 9, wherein the program instructions, when executed by the one or more computing devices, cause the one or more computing devices to:

compare a credential or an identity of an entity making the request with a directory of entities and/or credentials authorized to be provided the representation of the stored copy of the data captured by the camera,

wherein said providing the representation of the stored copy of the data captured by the camera is performed in response to determining a match between the credential and/or the identity of the entity making the request with a given credential and/or a given entity included in the directory.

14. The system of claim 13, wherein the program instructions, when executed by the one or more computing devices, cause the one or more computing devices to:

receive updates from an owner of the data captured by the camera stored in the secure storage repository regarding entities and/or credentials authorized to be provided the representation of the stored copy of the data captured by the camera; and

update the directory based on the owner provided updates.

15. The system of claim 13, wherein the program instructions, when executed by the one or more computing devices, cause the one or more computing devices to:

- receive updates from the mobile electronic device indicating images that have been authorized for public sharing; and
- update the directory to allow representations of image data for the images authorized for public sharing to be provided in response to authentication requests.

16. The system of claim 13, wherein the program instructions, when executed by the one or more computing devices, cause the one or more computing devices to:

- receive social media relationship information indicating entities having a relationship with an owner of the data captured by the camera stored in the secure storage repository; and
- provide the representation of the stored copy of the data captured by the camera in response to an authentication request, wherein a determination to provide the representation is based on a given relationship between a requestor of the authentication request and the owner as indicated in the social media relationship information.

17. The system of claim 9, wherein a signed token is received via the secure communication channel with the copy of the data captured by the camera, wherein the signed token is appended to the data by an image signal processor of the mobile electronic device, and

wherein the program instructions when executed by the one or more computing devices, cause the one or more computing devices to:

- authenticate the copy of the data captured by the camera as coming from a particular mobile electronic device which has been issued cryptographic information for generating the signed token.

18. The system of claim 9, wherein the program instructions, when executed by the one or more computing devices, cause the one or more computing devices to:

- generate a hash of the received copy of the data captured by the camera of the mobile electronic device;
- store the hash in the secure storage repository with the copy of the data captured by the camera of the mobile electronic device; and
- verify using the stored hash, prior to providing the representation of the stored copy of the data captured by the camera, that the stored copy of the data captured by the camera has not been altered.

19. The system of claim 9, wherein the copy of the data captured by the camera comprises one or more of:

- an image;
- a video; or
- volumetric visual content.

20. One or more non-transitory, computer-readable, storage media, storing program instructions that, when executed using one or more processors, cause the one or more processors to:

- forward image data and an appended identifier to a secure storage repository, wherein the image data and the appended identifier are forwarded to the secure storage repository using a secure communication channel implemented at an OS layer below an application layer such that the secure communication channel is not accessible to applications executing at the application layer.