CLAIMS

1. A method for protection of data across multiple users and devices, comprising:

in privacy server comprising at least one computer processor:

receiving, from a first user device, an initial data sharing permission for the first user device and a data sharing permission for a second user device, the first user device and the second user device associated with the same user;

provisioning the data sharing permission for the second user device;

communicating the provisioned data sharing permission to the second user device, wherein the second user device shares data with the first user device according to the provisioned data sharing permission**;**

receiving, from the first user device, an updated data sharing permission for the second user device;

determining that the updated data sharing permission for the second user device is different from the initial data sharing permission;

in response to the determination, communicating the updated data sharing permission to the second user device;

receiving, from the first user device, a third data sharing permission for the second user device and a third user device, the first user device and the third user device associated with the same user;

determining that the third data sharing permission does not change the updated data sharing permission for the second user device; and

communicating the third data sharing permission to the third user device and not to the second user device.

2. The method of claim 1, wherein the data sharing permission identifies a type of data to share.

3. The method of claim 2, wherein the type of data includes at least one of account data, activity data, and preference data.

4. The method of claim 1, wherein the first user device is associated with a first device key and the second user device is associated with a second device key, and the second device is identified to the privacy server by the second device key.

5. The method of claim 1, further comprising:

receiving encrypted data from the first user device or the second user device; and

storing the encrypted data in accordance with the data sharing permission.

6. The method of claim 5, further comprising:

communicating the encrypted data to the first user device or the second user device in accordance with the data sharing permission.

7. The method of claim 5, further comprising:

restoring the encrypted data to the same user device from which it originated.

8. A method for sharing data among devices associated with a plurality of users, comprising:

in privacy server comprising at least one computer processor:

receiving, from a first privacy application executed on a first electronic device, registration for a first user, wherein the registration comprises an identification of the first user device and an identification of a data owner for the data on the first user device;

receiving, from the first privacy application, data sharing preferences for the first user;

saving the data sharing preferences for the first user;

receiving, from a second privacy application executed on a second electronic device, registration for a second user, wherein the registration comprises an identification of the second user device and an identification of a data owner for the data on the second user device;

receiving, from the first privacy application, a request for the second user to share data with the first user;

communicating the request to the second privacy application;

receiving, from the second privacy application, a response to the request, wherein the response approves or denies the request;

configuring data sharing permissions for the first device and the second device;

communicating the data sharing permissions to the first privacy application and to the second privacy application, wherein at least one of the first privacy application and the second privacy application update data sharing permissions on the respective device;

receiving, from the first privacy application, updated data sharing preferences for the first user;

determining that the updated data sharing preferences alter the data sharing permissions with the second device;

in response to the determination, updating the data sharing permissions with the second device;

communicating the updated data sharing permissions to the second privacy application;

receiving, from the privacy application, a data sharing permission for the second device and a third device, the first device and the third device associated with the same user;

determining that the data sharing permission does not change the updated data sharing permissions for the second device; and

communicating the data sharing permission to the third user device and not to the second user device.

9. The method of claim 8, wherein the request for the second user to share data with the first user identifies a type of data to share.

10. The method of claim 9, wherein the type of data includes at least one of account data, activity data, and preference data.

11. The method of claim 8, further comprising:

receiving encrypted data from the first user device or the second user device; and

storing the encrypted data in accordance with the data sharing permissions.

12. The method of claim 11, further comprising:

communicating the encrypted data to the first user device or the second user device in accordance with the data sharing permissions.

13. A method for sharing data among devices associated with a plurality of users, comprising:

in privacy server comprising at least one computer processor:

receiving, from a first privacy application executed on a first electronic device, registration for a first user, wherein the registration comprises an identification of the first user device and an identification of a data owner for the data on the first user device;

receiving, from the first privacy application, data sharing preferences for the first user;

saving the data sharing preferences for the first user;

receiving, from a second privacy application executed on a second electronic device, registration for a second user, wherein the registration comprises an identification of the second user device and an identification of a data owner for the data on the second user device;

receiving, from the second privacy application, a request for the second user to share data with the first user;

configuring data sharing permissions for the first device and the second device;

communicating the data sharing permissions to the first privacy application and to the second privacy application, wherein at least one of the first privacy application and the second privacy application update data sharing permissions on the respective device;

receiving, from the first privacy application, updated data sharing preferences for the first user;

determining that the updated data sharing preferences alter the data sharing permissions with the second device;

in response to the determination, updating the data sharing permissions with the second device;

communicating the updated data sharing permissions to the second privacy application;

receiving, from the first privacy application, a data sharing permission for the second device and a third device, the first device and the third device associated with the same first user;

determining that the data sharing permission does not change the updated data sharing permissions for the second device; and

communicating the data sharing permission to the third user device and not to the second user device.

14. The method of claim 13, wherein the request for the second user to share data with the first user identifies a type of data to share.

15. The method of claim 14, wherein the type of data includes at least one of account data, activity data, and preference data.

16. The method of claim 13, further comprising:

receiving encrypted data from the first user device or the second user device; and

storing the encrypted data in accordance with the data sharing permissions.

17. The method of claim 8, further comprising:

receiving, from the first privacy application, second updated data sharing preferences for the first user;

determining that the updated data sharing preferences do not alter the data sharing permissions with the second device; and

in response to the determination, declining to communicate the second updated data sharing preferences to the second privacy application.

18. The method of claim 13, further comprising:

receiving, from the first privacy application, second updated data sharing preferences for the first user;

determining that the updated data sharing preferences do not alter the data sharing permissions with the second device; and

in response to the determination, declining to communicate the second updated data sharing preferences to the second privacy application.