

CLAIMS

What is claimed is:

1. A method for federated privacy management, comprising:
receiving, at a user management node, and from a client application executing on an electronic device, a device identifier;
receiving, by the user management node, and from a second layer node in a multi-layer federated privacy management network, data comprising at least one of browsing data and application data from a web host or a server, wherein the data is in response to an internet protocol request from the client application via a first layer node and the second layer node to the web host or the server, and the data is associated with the device identifier;
receiving, at the user management node, a request for the data from the client application using the device identifier; and
communicating the data to the client application.
2. The method of claim 1, wherein the data from the second layer node comprises at least one of browsing data and application data from the web host or the server.
3. The method of claim 1, wherein the first layer node receives the internet protocol request and a first IP address associated with the electronic device from the client application, translates the first IP address into a second IP address, and communicates the internet protocol request and the second IP address to the second layer node.
4. The method of claim 3, wherein the second layer node executes a privacy service on the internet protocol request.

5. The method of claim 4, wherein the privacy service comprises at least one of packet inspection, device fingerprint obfuscation, web security, an anti-malware application activity, and logging of browsing/application history.
6. The method of claim 3, wherein the second layer node translates the second IP address into a third IP address and communicates the internet protocol request and the third IP address to the web host or the server.
7. The method of claim 1, wherein the data is encrypted with a private key for the client application.
8. The method of claim 1, wherein the second layer node comprises a plurality of second layer nodes.
9. The method of claim 1, further comprising:
 - receiving, at the user management node, registration information from the client application;
 - requesting, by the user management node, an entitlement token from the first layer node or the second layer node;
 - receiving, from the user management node and from the first layer node or the second layer node, the entitlement token; and
 - communicating, by the user management node, the entitlement token to the client application, wherein the client application registers with the first layer node or the second layer node with the entitlement token.
10. A method for federated privacy management, comprising:
 - receiving, by a user management node, data from a second layer node in a multi-layer federated privacy management network, the data associated with a session identifier, wherein the data is in response to an internet protocol request

from a client application via a first layer node and the second layer node to a web host or a server;

receiving, at the user management node, a request for the data from a client application using the session identifier; and
communicating the data to the client application.

11. The method of claim 10, wherein the data from the second layer node comprises at least one of browsing data and application data from the web host or the server.

12. The method of claim 10, wherein the first layer node receives the internet protocol request and a first IP address associated with an electronic device from the client application, replaces the first IP address with a second IP address, and communicates the internet protocol request and the second IP address to the second layer node.

13. The method of claim 12, wherein the second layer node executes a privacy service on the internet protocol request.

14. The method of claim 13, wherein the privacy service comprises at least one of packet inspection, device fingerprint obfuscation, web security, an anti-malware application activity, and logging of browsing/application history.

15. The method of claim 12, wherein the second layer node replaces the second IP address with a third IP address and communicates the internet protocol request and the third IP address to the web host or the server.

16. The method of claim 10, wherein the data is encrypted with a private key for the client application.

17. The method of claim 10, further comprising:
receiving, at the user management node, registration information from the client application;
requesting, by the user management node, an entitlement token from the first layer node or the second layer node;
receiving, from the user management node and from the first layer node or the second layer node, the entitlement token; and
communicating, by the user management node, the entitlement token to the client application, wherein the client application registers with the first layer node or the second layer node with the entitlement token.

18. A system for federated privacy management, comprising:
a multi-layer federated privacy management network comprising a first layer node and a second layer node;
a user management node in communication with at least one of the first layer node and the second layer node; and
a client application executed by an electronic device;
wherein:
the user management node receives, from the client application, a device identifier for the electronic device;
the first layer node receives an internet protocol request and a first IP address associated with the electronic device from the client application, translates the first IP address into a second IP address, and communicates the internet protocol request and the second IP address to the second layer node;
the second layer node translates the second IP address into a third IP address and communicates the internet protocol request and the third IP address to a web host or a server;

the second layer node receives data comprising at least one of browsing data and application data from the web host or the server and associates it with the device identifier or a session identifier and communicates the data and the association with the device identifier or the session identifier to the user management node;

the user management node receives the data and stores the data;

the user management node receives a request for the data from the client application using the device identifier or the session identifier; and

the user management node communicates the data to the client application.

19. The system of claim 18, wherein the second layer node further executes a privacy service comprising at least one of packet inspection, device fingerprint obfuscation, web security, an anti-malware application activity, and logging of browsing/application history on the internet protocol request.

20. The system of claim 18, further comprising a plurality of second layer nodes.