WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by an identity and profiling system, a request from an entity computing system for a first set of information associated with a user, the first set of information corresponding to personally identifiable information that is being requested by the entity computing system;

sending, by the identity and profiling system, a request to a mobile device operated by the user for the first set of information associated with the user;

receiving, by the identity and profiling system, an access token from the mobile device, the access token having been generated by encrypting a second set of information using a key associated with the user, the second set of information indicating a set of personally identifiable information for the user that the user is permitting to be released to the entity computing system;

determining, by the identity and profiling system, the key associated with the user;

decrypting, by the identity and profiling system, the access token using the key in order to obtain the second set of information associated with the user;

determining from a main blockchain, by the identity and profiling system, at least one storage location for a third set of information associated with the user, the third set of information corresponding to the actual values for the personally identifiable information that the user is permitting to be released to the entity computing system;

locating, by the identity and profiling system, the third set of information associated with the user in an offchain based on the at least one storage location; and

sending, by the identity and profiling system, the third set of information associated with the user to the entity computing system,

wherein the offchain stores the personally identifiable information for the user in a distributed manner without storing any information of which user the personally identifiable information is associated with so that the personally identifiable information

is stored by the offchain in an anonymized manner to provide an extra layer of security, the main blockchain storing the various locations where the personally identifiable information for the user is stored in the offchain.

2. The method of claim 1, wherein the offchain is a decentralized data store.

3. The method of claim 1, wherein the offchain is an alternate blockchain.

4. The method of claim 1, wherein the at least one storage location for the third set of information associated with the user is indicated in a smart contract of the main blockchain.

5. The method of claim 1, wherein the method further comprises:

determining, by the identity and profiling system, that a phone number for a mobile device associated with the user exists within the identity and profiling system.

6. The method of claim 1, wherein the method further comprises:

determining, by the identity and profiling system, that a phone number for a mobile device associated with the user does not exist within the identity and profiling system;

upon determining that the phone number for a mobile device associated with the user does not exist within the identity and profiling system, sending, by the identity and profiling system, a request to the mobile device for the user to provide the first set of information associated with the user;

assigning, by the identity and profiling system, the key associated with the user to the mobile device;

receiving, by the identity and profiling system, the first set of information associated with the user from the mobile device; and

storing, by the identity and profiling system, the first set of information associated with the user in the offchain, wherein at least one storage location for the first set of information associated with the user is stored in the main blockchain.

7. A computing system comprising:

a state data store;

a processor;

a computer-readable memory containing program instructions that, when executed by the processor, cause the processor to:

receive a request from an entity computing system for a first set of information associated with a user, wherein the entity computing system is associated with an entity identifier and the first set of information corresponding to personally identifiable information that is being requested by the entity computing system;

send a request to a mobile device operated by the user for the first set of information associated with the user;

receive an access token from the mobile device, the access token having been generated by encrypting a second set of information using a key associated with the user, the second set of information indicating a set of personally identifiable information for the user that the user is permitting to be released to the entity computing system;

determine the key associated with the user;

decrypt the access token using the key in order to obtain the second set of information associated with the user;

determine, from a main blockchain, at least one storage location for a third set of information associated with the user, the third set of information corresponding to the actual values for the personally identifiable information that the user is permitting to be released to the entity computing system;

locate the third set of information associated with the user in an offchain based on the at least one storage location; and

send the third set of information associated with the user to the entity computing system,

wherein the offchain stores the personally identifiable information for the user in a distributed manner without storing any information of which user the personally identifiable information is associated with so that the personally identifiable information is stored by the offchain in an anonymized manner to provide an extra layer of security, the main blockchain storing the various locations where the personally identifiable information for the user is stored in the offchain.

8. The computing system of claim 7, wherein the offchain is a decentralized data store.

9. The computing system of claim 7, wherein the offchain is an alternate blockchain.

10. The computing system of claim 7, wherein the at least one storage location for the third set of information associated with the user is indicated in a smart contract of the main blockchain.

11. The computing system of claim 7, wherein the program instructions, when executed by the processor, further cause the processor to:

determine that a phone number for a mobile device associated with the user exists within the state data store.

12. The computing system of claim 7, wherein the program instructions, when executed by the processor, further cause the processor to:

determine that a phone number for a mobile device associated with the user does not exist within the state data store;

upon determining that the phone number for a mobile device associated with the user does not exist within the state data store, send a request to the mobile device for the user to provide the first set of information associated with the user;

assign the key associated with the user to the mobile device;

receive the first set of information associated with the user from the mobile device; and

store the first set of information associated with the user in the offchain, wherein at least one storage location for the first set of information associated with the user is stored in the main blockchain.