WHAT IS CLAIMED IS:

1. A method comprising:

receiving a request from a user to access data that was acquired by a third-party from a data owner, the data in an encrypted format unreadable by the user;

in response to receiving the request from the user to access the data:

requesting a third-party key from the third-party; and

requesting, by a security appliance of the user, a data owner key from the data owner, the requesting a data owner key from the data owner comprising communicating with a security appliance of the data owner to request the data owner key, wherein the security appliance of the data owner returns the data owner key in response to determining that the data owner authorizes the user to have access to the data, thereby providing the data owner with control of access to the data after the data has been acquired by the third-party; and

in response to receiving the third-party key and the data owner key:

applying the third-party key and the data owner key to the data in the encrypted format to generate the data in an unencrypted format readable by the user; and

providing the user with access to the data in the unencrypted format.

2. The method of claim 1, wherein the requesting a third-party key from the third-party comprises communicating with a security appliance of the third-party to request the third-party key, wherein the security appliance returns the third-party key in response to determining that the third-party authorizes the user to have access to the data.

3. The method of claim 1, wherein the third-party is a data broker.

~~4. The method of claim 1, wherein the requesting a data owner key from the data owner comprises communicating with a security appliance of the data owner to request the data owner key, wherein the security appliance returns the data owner key~~

~~in response to determining that the data owner authorizes the user to have access to the data.~~

~~5~~4. The method of claim 1, wherein the encrypted format of the data was generated by encrypting the data using the data owner key and encrypting the data encrypted using the data owner key using the third-party key.

~~6~~5. The method of claim 1, further comprising in response to receiving the request from the user to access the data, logging the request from the user to access the data.

~~7~~6. The method of claim 1, further comprising in response to providing the user with access to the data in the unencrypted format, logging the providing the user with access to the data in the unencrypted format.

~~8~~7. The method of claim 1, wherein the data in the unencrypted format includes at least a subset of the data being masked or redacted.

~~9~~8. A system comprising:

one or more processors for executing computer readable instructions, the computer readable instructions controlling the one or more processors to perform operations comprising:

receiving a request from a user to access data that was acquired by a third-party from a data owner, the data in an encrypted format unreadable by the user;

in response to receiving the request from the user to access the data:

requesting a third-party key from the third-party; and

requesting, by a security appliance of the user, a data owner key from the data owner, the requesting a data owner key from the data owner comprising communicating with a security appliance of the data owner to request the data owner key, wherein the security appliance of the data owner returns the data owner key in response to determining that the data owner authorizes the user to have access to the data, thereby providing the data owner with control of access to the data after the data has been acquired by the third-party; and

in response to receiving the third-party key and the data owner key:

applying the third-party key and the data owner key to the data in the encrypted format to generate the data in an unencrypted format readable by the user; and

providing the user with access to the data in the unencrypted format.

~~10~~9. The system of claim ~~9~~8, wherein the requesting a third-party key from the third-party comprises communicating with a security appliance of the third-party to request the third-party key, wherein the security appliance returns the third-party key in response to determining that the third-party authorizes the user to have access to the data.

~~11~~10. The system of claim ~~9~~8, wherein the third-party is a data broker.

~~12. The system of claim 9, wherein the requesting a data owner key from the data owner comprises communicating with a security appliance of the data owner to request the data owner key, wherein the security appliance returns the data owner key in response to determining that the data owner authorizes the user to have access to the data.~~

~~13~~11. The system of claim ~~9~~8, wherein the encrypted format of the data was generated by encrypting the data using the data owner key and encrypting the data encrypted using the data owner key using the third-party key.

~~14~~12. The system of claim ~~9~~8, wherein the operations further comprise, in response to receiving the request from the user to access the data, logging the request from the user to access the data.

~~15~~13. The system of claim ~~9~~8, wherein the operations further comprise, in response to providing the user with access to the data in the unencrypted format, logging the providing the user with access to the data in the unencrypted format.

~~16~~14. The system of claim ~~9~~8, wherein the data in the unencrypted format includes at least a subset of the data being masked or redacted.

~~17~~15. A computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

receiving a request from a user to access data that was acquired by a third-party from a data owner, the data in an encrypted format unreadable by the user;

in response to receiving the request from the user to access the data:

requesting a third-party key from the third-party; and

requesting, by a security appliance of the user, a data owner key from the data owner, the requesting a data owner key from the data owner comprising communicating with a security appliance of the data owner to request the data owner key, wherein the security appliance of the data owner returns the data owner key in response to determining that the data owner authorizes the user to have access to the data, thereby providing the data owner with control of access to the data after the data has been acquired by the third-party; and

in response to receiving the third-party key and the data owner key:

applying the third-party key and the data owner key to the data in the encrypted format to generate the data in an unencrypted format readable by the user; and

providing the user with access to the data in the unencrypted format.

~~18~~16. The computer program product of claim ~~17~~15, wherein the requesting a third-party key from the third-party comprises communicating with a security appliance of the third-party to request the third-party key, wherein the security appliance returns

the third-party key in response to determining that the third-party authorizes the user to have access to the data.

~~19. The computer program product of claim 17, wherein the requesting a data owner key from the data owner comprises communicating with a security appliance of the data owner to request the data owner key, wherein the security appliance returns the data owner key in response to determining that the data owner authorizes the user to have access to the data.~~

~~20~~17. The computer program product of claim ~~17~~15, wherein the encrypted format of the data was generated by encrypting the data using the data owner key and encrypting the data encrypted using the data owner key using the third-party key.