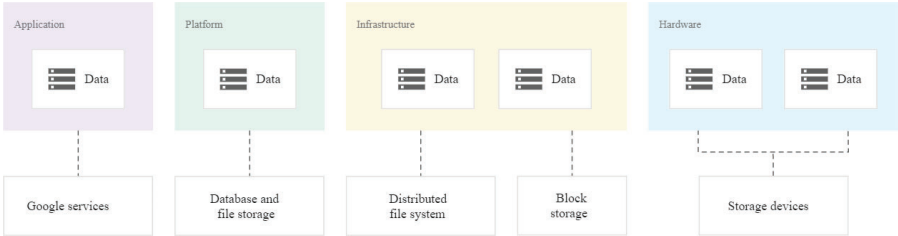


CHART C – U.S. PATENT NO. 11,178,116

U.S. Patent No. 11,178,116	Google’s “Encryption at Rest” ¹
Claim 1[pre] A method for securing a data set, the method comprising:²	Google’s “Encryption at Rest” practices a method for securing a data set. For example, Google states its “comprehensive security strategy includes encryption at rest,” and that it “encrypt[s] <i>all Google customer content at rest</i>, without any action required by” the customer. SFI-GOOGLE_000003146, <i>Default encryption at rest</i>, GOOGLE CLOUD (emphasis added). “Google encrypts all customer content stored at rest, without any action from you, using one or more encryption mechanisms. The following sections describe the mechanisms that we use to encrypt customer content.” <i>Id</i>; see also SFI-GOOGLE_000005743, <i>Cloud Key Management Service deep dive</i>, GOOGLE CLOUD (last visited Aug. 14, 2023), https://cloud.google.com/docs/security/key-management-deep-dive (Cloud Key Management Service). Google securely stores a data set using “several layers of encryption that are generally used to protect user data in Google production data centers,” SFI-GOOGLE_000003146 at -148, as seen in the image below.  <i>Id.</i>

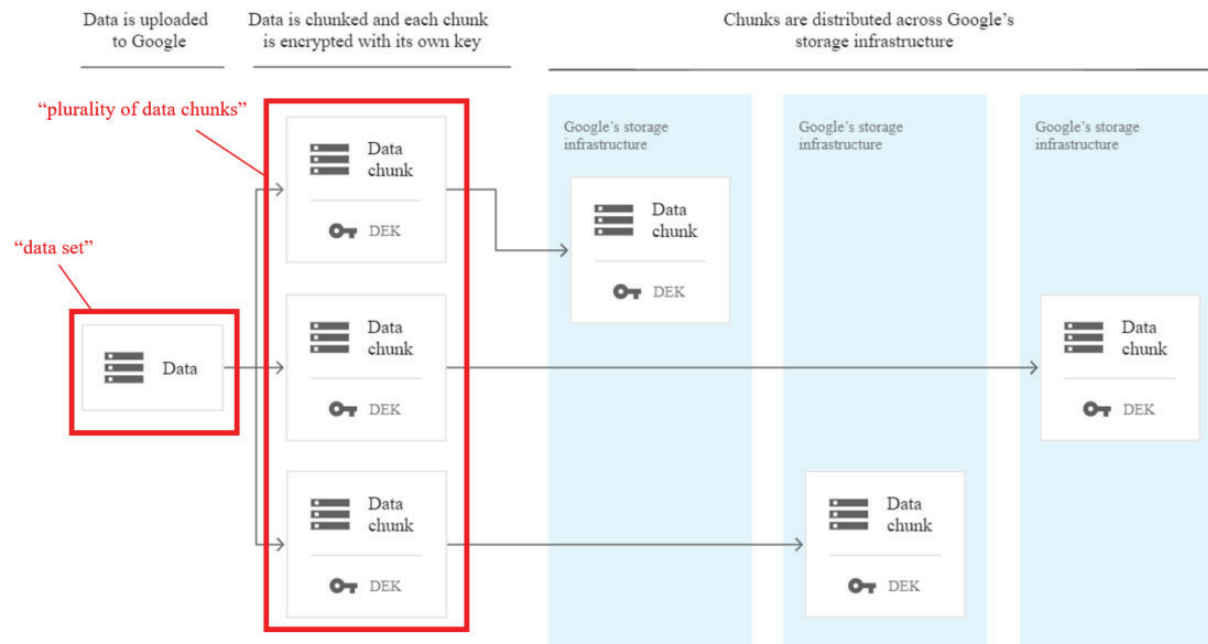
¹ As explained in more detail in the body of SFI’s response to Interrogatory No. 7, each of the Accused Services stores customer data using the accused “Encryption at Rest” technology, and, on that basis, infringes.

² Unless otherwise indicated, SFI contends that each element of every asserted claim of the ’116 Patent is literally present in the “Encryption at Rest” utilized by each of the Accused Services. To the extent any element is not literally infringed, SFI contends such element is infringed under the doctrine of equivalents.

1[a] distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;

Google's "Encryption at Rest" comprises distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set.

For example, Google distributes the data set into a plurality of data chunks by splitting the user data. *See* SFI-GOOGLE_000003146 at -153 ("Data is broken into subfile chunks for storage"); *see also* SFI-GOOGLE_000005743 (Cloud Key Management Service). Below is an exemplary annotated image from the Google Cloud webpage showing an example of a data set and a plurality of data chunks³:



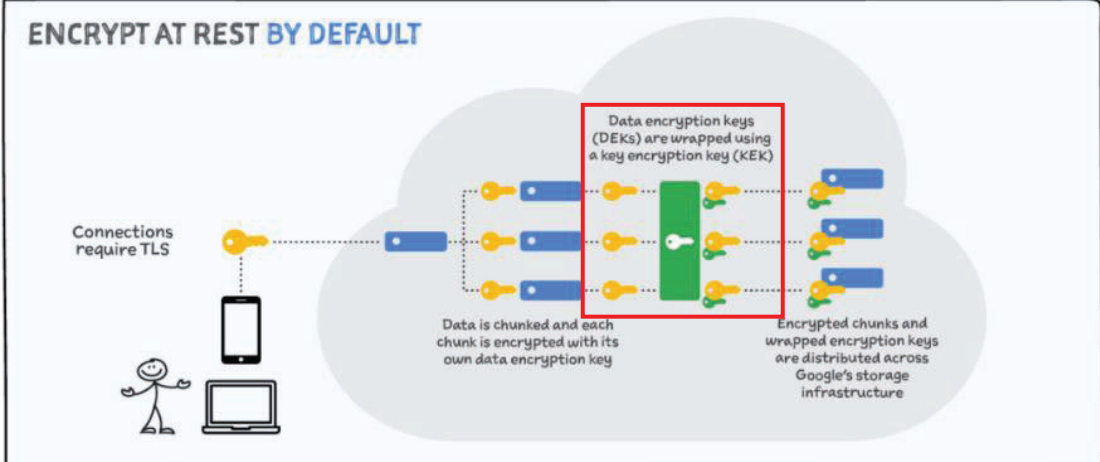
SFI-GOOGLE_000003146 at -149.

Further, none of the data chunks are, by themselves, sufficient to reconstruct the data set. For example, Google explains that "[a]n attacker who wants to access customer data would need to know and be able to access two things: all of the storage chunks that correspond to the data that they want and all of the encryption keys that correspond to the chunks." SFI-GOOGLE_000003146 at -153; *see also* SFI-GOOGLE_000003287 at -293 (the decryption of "all the chunks that compose a specific file or data" is

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	required before the data is made available to the requesting application.); SFI-GOOGLE_000005997, Google Cloud Tech, <i>How Google Protects Your Data at Rest and in Transit (Cloud Next '18)</i> , YOUTUBE (Aug. 17, 2018), https://www.youtube.com/watch?v=vxMwuL0hX3U&t=311s .
1[b] encrypting each of the data chunks with a respective one of a plurality of encryption keys;	Google's "Encryption at Rest" comprises encrypting each of the data chunks with a respective one of a plurality of encryption keys. For example, Google states that "[e]ach chunk is encrypted at the storage level with an individual data encryption key (DEK): two chunks won't have the same DEK, even if they are owned by the same customer or stored on the same machine." SFI-GOOGLE_000003146 at -148. Google explains that "[t]he storage system generates DEKs using Google's common cryptographic library. In general, DEK[s] are then sent to Keystore to wrap with that storage system's KEK, and the wrapped DEKs are passed back to the storage system to be kept with the data chunks." <i>Id.</i> at -151; <i>see also</i> SFI-GOOGLE_000005743 (Cloud Key Management Service). Below is an exemplary annotated image from the Google Cloud webpage showing examples of the plurality of encryption keys:

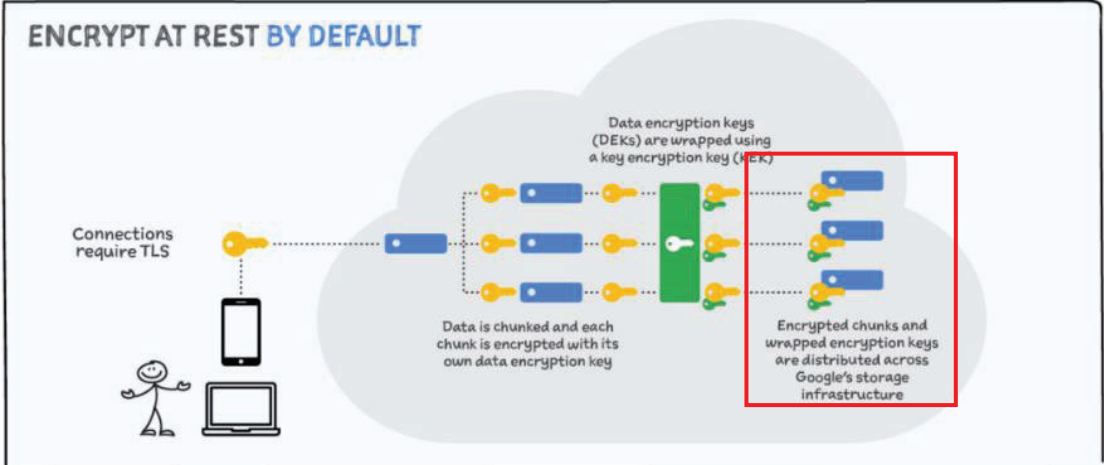
³ The red boxes and accompanying text are annotations added by SFI for purposes of this claim chart.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	The diagram illustrates the process of Google's "Encryption at Rest": Data is uploaded to Google: A box labeled "Data" is shown. Data is chunked and each chunk is encrypted with its own key: The data is split into three "Data chunk" boxes. Each chunk is associated with its own "DEK" (Data Encryption Key), represented by a key icon. Chunks are distributed across Google's storage infrastructure: Three vertical blue bars represent "Google's storage infrastructure". Each chunk and its corresponding DEK are distributed to a separate storage location. Annotation: A red arrow points from the text "plurality of encryption keys" to the three individual DEKs, highlighting that each chunk has a unique key.
1[c] obfuscating each of the plurality of different encryption keys; and	SFI-GOOGLE_000003146 at -149. Google's "Encryption at Rest" comprises obfuscating each of the plurality of different encryption keys. For example, Google obfuscates each of the different encryption keys when it encrypts the DEKs using the KEKs. Google explains that "DEKs are encrypted with (wrapped by) a key encryption key (KEK)." SFI-GOOGLE_000003146 at -149.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	Below is an exemplary annotated image showing Google's obfuscation of the DEKs by the KEKs.⁴ 
1[d] separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.	Google's "Encryption at Rest" comprises separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices. For example, after the original data is split and encrypted, each encrypted chunk is stored in a storage system with its data encryption key.⁵ SFI-GOOGLE_000003146 at -151 ("[W]rapped DEKs are passed back to the storage system to be kept with the data chunks."). Google explains that "[b]ecause of the high volume of keys at Google, and the need for low latency and high availability, DEKs are stored near the data that they

⁴ SFI-GOOGLE_000005816, *Data security in Google Cloud*, GOOGLE CLOUD: BLOG (July 20, 2022), <https://cloud.google.com/blog/topics/developers-practitioners/data-security-google-cloud>.

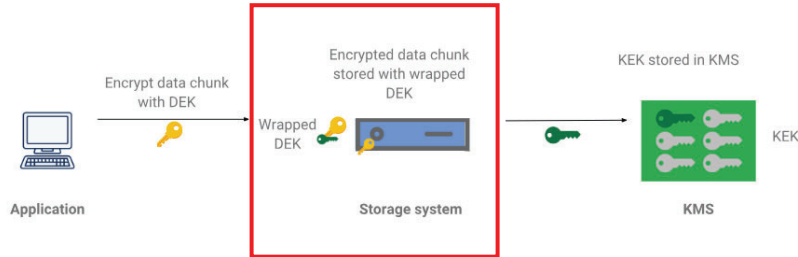
⁵ SFI-GOOGLE_000005992, Google Cloud Tech, *How does encryption work at Google's data centers?*, YOUTUBE (Nov. 24, 2021), <https://www.youtube.com/watch?v=82YD6esAK0o>.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	encrypt." SFI-GOOGLE_000003146 at -150; <i>see also</i> SFI-GOOGLE_000005743 (Cloud Key Management Service).⁶ Google explains that "[e]ach chunk is distributed across our storage systems and is replicated in encrypted form for backup and disaster recovery." SFI-GOOGLE_000003146 at -149. Google explains that chunks of data are stored with their own DEK and are "stored across multiple servers."⁷ Below is an annotated image showing Google's distribution of data chunks and DEKs across Google's storage infrastructure.⁸  The diagram, titled "ENCRYPT AT REST BY DEFAULT", illustrates the data flow and encryption process. On the left, a stick figure represents a user with a smartphone and a laptop. A dashed line labeled "Connections require TLS" connects the user to a cloud representing Google's infrastructure. Inside the cloud, a central green box represents the key management system. To the left of this box, several blue rectangles represent data chunks, each connected to a yellow key icon representing a Data Encryption Key (DEK). A label states: "Data is chunked and each chunk is encrypted with its own data encryption key". To the right of the green box, several yellow key icons represent wrapped DEKs, connected to a label: "Data encryption keys (DEKs) are wrapped using a key encryption key (KEK)". On the far right, a red box highlights a set of blue rectangles (encrypted chunks) and yellow key icons (wrapped DEKs), with a label: "Encrypted chunks and wrapped encryption keys are distributed across Google's storage infrastructure".

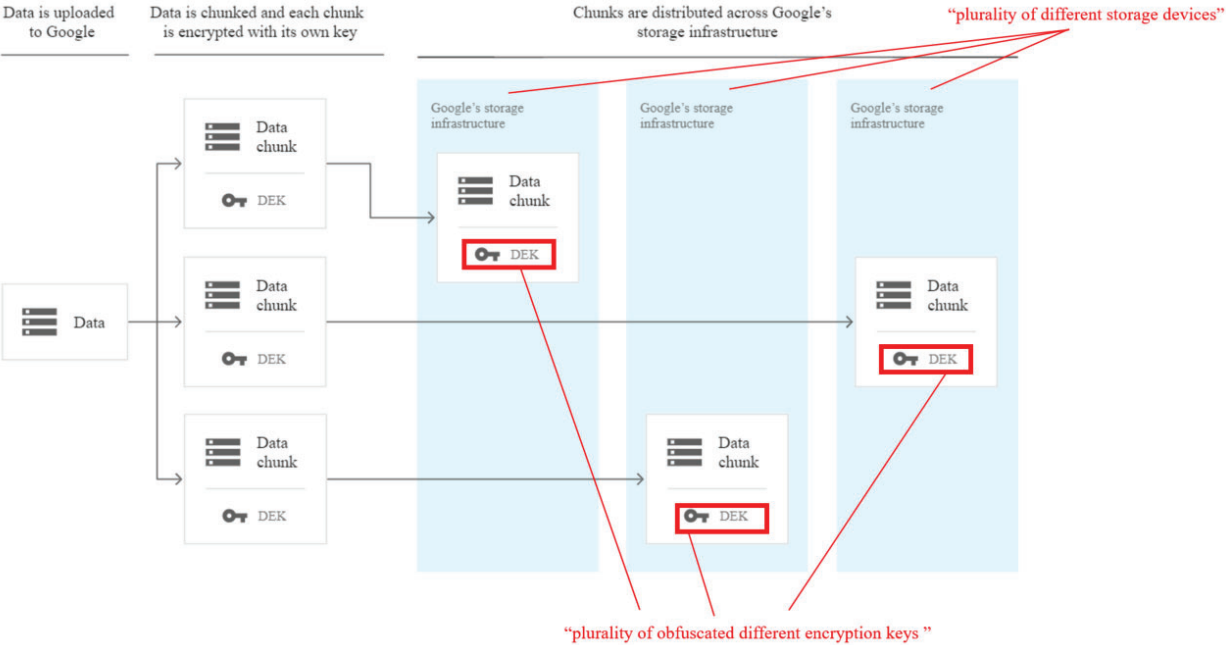
⁶ *See also* SFI-GOOGLE_000005933, Google Cloud Tech, *Google Cloud Encryption at Rest*, YouTube (Dec. 12, 2017) <https://www.youtube.com/watch?v=Svz2KHE1mdM>.

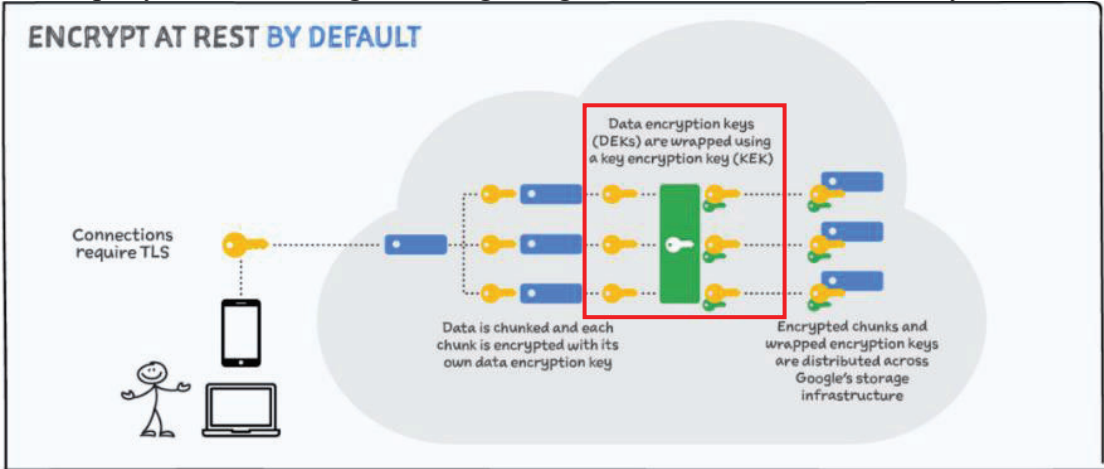
⁷ SFI-GOOGLE_000005992; *see also* SFI-GOOGLE_000005803, *Data and Security*, GOOGLE DATA CENTERS (last visited Aug. 14, 2023), <https://www.google.com/about/datacenters/data-security/> ("Rather than storing each user's data on a single machine or set of machines, we distribute all data . . . across many computers in different locations.").

⁸ SFI-GOOGLE_000005816.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	As another example, below is an image from Google Cloud's webpage illustrating that every encrypted chunk is stored with its wrapped DEK.⁹  Below is an exemplary annotated image from the Google Cloud webpage showing an example of the plurality of different storage devices and the obfuscated different encryption keys stored with the data chunks:

⁹ SFI-GOOGLE_000005887, *Envelope encryption*, GOOGLE CLOUD (last visited Aug. 14, 2023), <https://cloud.google.com/kms/docs/envelope-encryption>.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	 The diagram illustrates Google's "Encryption at Rest" process. It begins with "Data is uploaded to Google", which is then "chunked and each chunk is encrypted with its own key". The resulting "Data chunk" and "DEK" (Data Encryption Key) are then distributed across "Google's storage infrastructure". The infrastructure is composed of multiple "Google's storage infrastructure" blocks, representing a "plurality of different storage devices". Each block contains a "Data chunk" and a "DEK". The DEKs are highlighted with red boxes, indicating a "plurality of obfuscated different encryption keys". SFI-GOOGLE 000003146 at -149.
Claim 2[pre] The method of claim 1,	Google's "Encryption at Rest" comprises the method of claim 1. <i>See</i> Claim 1, <i>supra</i> .
2[a] wherein obfuscating each of the plurality of different encryption keys comprises performing a transform on data indicative of at least one of the plurality of different encryption keys.	Within Google's "Encryption at Rest," obfuscating each of the plurality of different encryption keys comprises performing a transform on data indicative of at least one of the plurality of different encryption keys. For example, Google performs a transform on each of the different encryption keys when it encrypts the DEKs using the KEKs. Google explains that "DEKs are encrypted with (wrapped by) a key encryption key

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	(KEK)." SFI-GOOGLE_000003146 at -149; <i>see also</i> SFI-GOOGLE_000005743 (Cloud Key Management Service).¹⁰ Below is an exemplary annotated image showing Google's transform on the DEKs by the KEKs.¹¹ 
Claim 5[pre] The method of claim 1,	Google's "Encryption at Rest" comprises the method of claim 1. <i>See</i> Claim 1, <i>supra</i> .

¹⁰ *See also* SFI-GOOGLE_000005933 ("[T]he data encryption keys are themselves encrypted with another key for storage, called the key encryption key.").

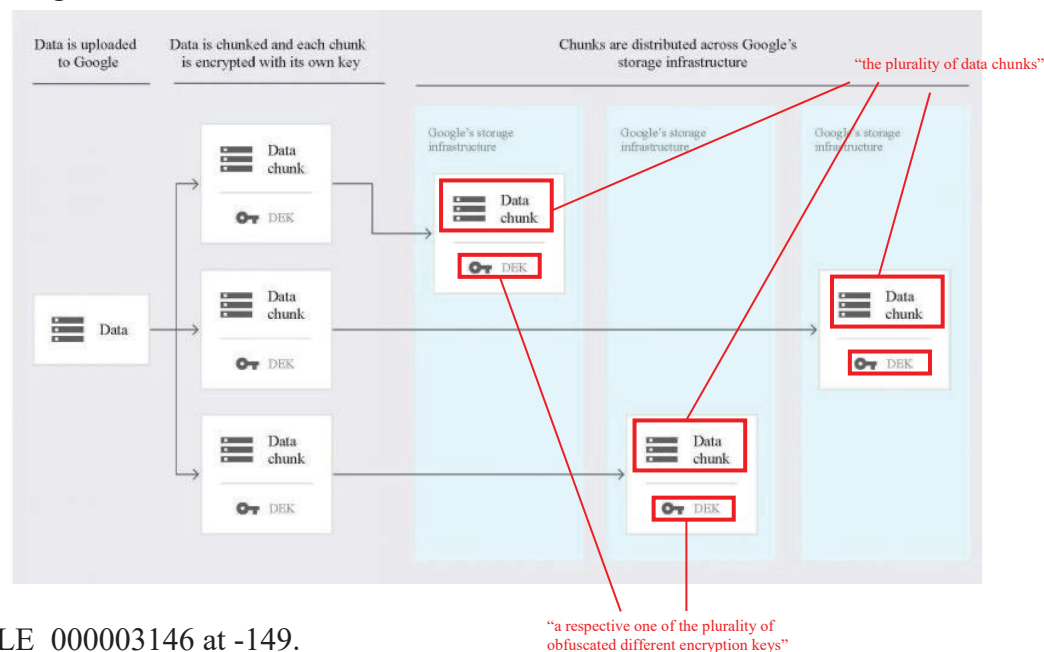
¹¹ SFI-GOOGLE_000005816.

5[a] wherein storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

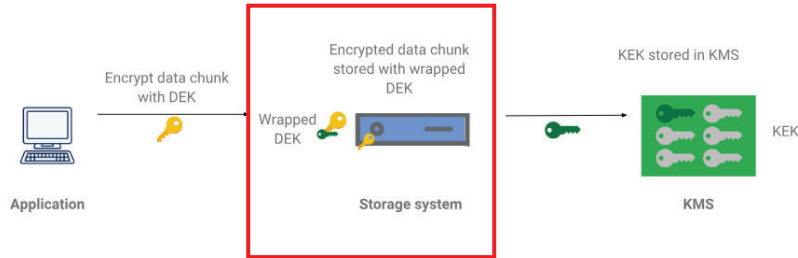
Within Google's "Encryption at Rest," storing the plurality of data chunks together with the plurality of obfuscated different encryption keys comprises storing each of the plurality of data chunks together with a respective one of the plurality of obfuscated different encryption keys.

For example, each obfuscated DEK is stored with the data chunk it encrypts. Google explains that "[t]he storage system generates DEKs using Google's common cryptographic library. In general, DEKS are then sent to Keystore to wrap with that storage system's KEK, and the wrapped DEKs are passed back to the storage system to be kept with the data chunks." SFI-GOOGLE_000003146 at -151. Google explains that "[b]ecause of the high volume of keys at Google, and the need for low latency and high availability, DEKs are stored near the data that they encrypt." SFI-GOOGLE_000003146 at -150; *see also* SFI-GOOGLE_000005743 (Cloud Key Management Service).

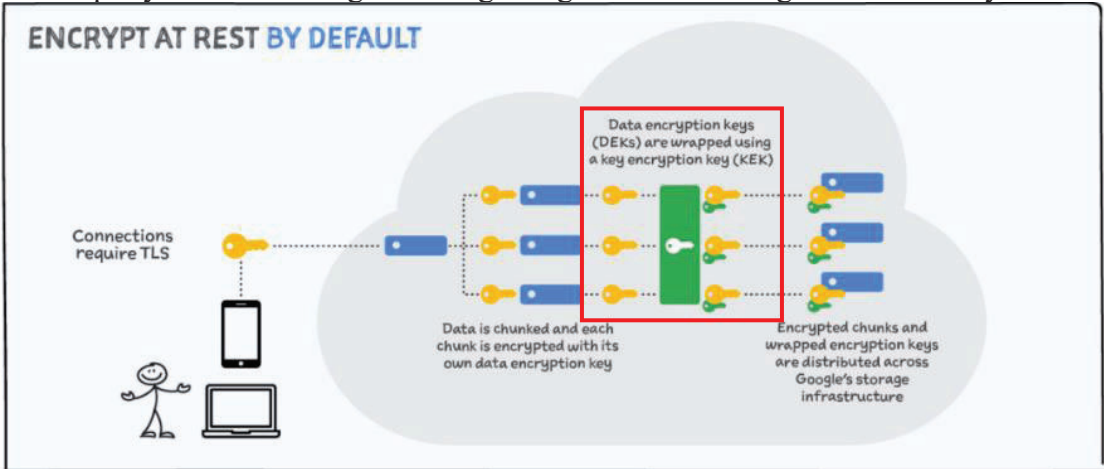
Below is an exemplary annotated image from the Google Cloud webpage showing how a DEK is stored with its corresponding data chunk:



SFI-GOOGLE_000003146 at -149.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	As another example, below is an image from Google Cloud's webpage illustrating that every encrypted chunk is stored with its wrapped DEK.¹² 
Claim 9[pre] A method for securing a data set, the method comprising:	Google's "Encryption at Rest" comprises a method for securing a data set. <i>See</i> Claim 1 [pre], <i>supra</i>.
9[a] distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;	Google's "Encryption at Rest" comprises distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set. <i>See</i> Claim 1[a], <i>supra</i>.
9[b] encrypting each of the data chunks with a respective one of a plurality of encryption keys;	Google's "Encryption at Rest" comprises encrypting each of the data chunks with a respective one of a plurality of encryption keys. <i>See</i> Claim 1[b], <i>supra</i>.

¹² SFI-GOOGLE_000005887.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
9[c] transforming each of the plurality of different encryption keys; and	Google's "Encryption at Rest" comprises transforming each of the plurality of different encryption keys. For example, Google transforms each of the different encryption keys when it encrypts the DEKs using the KEKs. Google explains that "DEKs are encrypted with (wrapped by) a key encryption key (KEK)." SFI-GOOGLE_000003146 at -149. Below is an exemplary annotated image showing Google's transforming of the DEKs by the KEKs.¹³ 

¹³ SFI-GOOGLE_000005816.

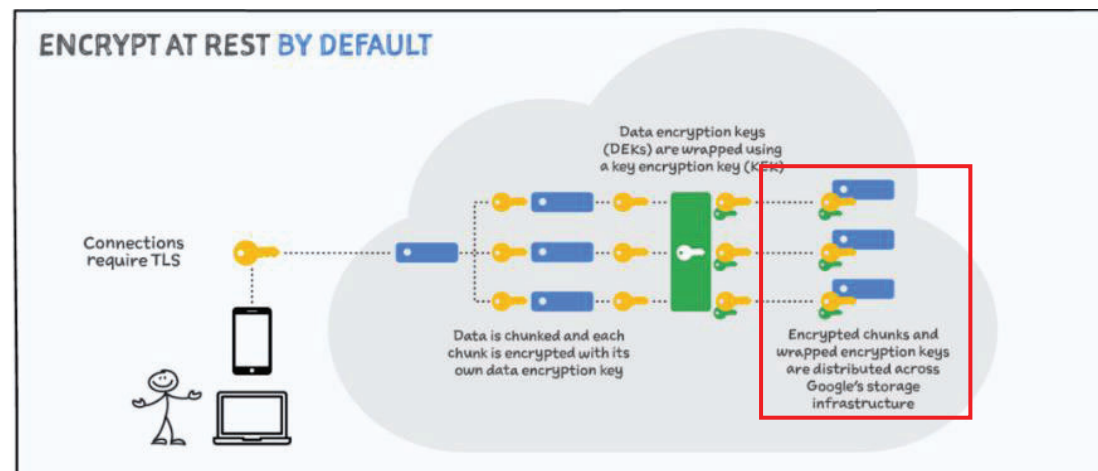
9[d] separately storing each data chunk of the plurality of data chunks together with one of the plurality of transformed different encryption keys on a plurality of different storage devices.

Google's "Encryption at Rest" comprises separately storing each data chunk of the plurality of data chunks together with one of the plurality of transformed different encryption keys on a plurality of different storage devices.

For example, after the original data is split and encrypted, each encrypted chunk is stored in a storage system with its data encryption key.¹⁴ SFI-GOOGLE_000003146 at -151 ("[W]rapped DEKs are passed back to the storage system to be kept with the data chunks."). Google explains that "[b]ecause of the high volume of keys at Google, and the need for low latency and high availability, DEKs are stored near the data that they encrypt." SFI-GOOGLE_000003146 at -150; *see also* SFI-GOOGLE_000005743 (Cloud Key Management Service).¹⁵

Google explains that "[e]ach chunk is distributed across our storage systems and is replicated in encrypted form for backup and disaster recovery." SFI-GOOGLE_000003146 at -149. Google explains that chunks of data are stored with their own DEK and are "stored across multiple servers."¹⁶

Below is an annotated image showing the distribution of data chunks and DEKs across Google's storage infrastructure.¹⁷



U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	As another example, below is an image from Google Cloud's webpage illustrating that every encrypted chunk is stored with its wrapped DEK.¹⁸  Below is an exemplary annotated image from the Google Cloud webpage showing an example of the plurality of different storage devices and the transformed different encryption keys stored with the data chunks:

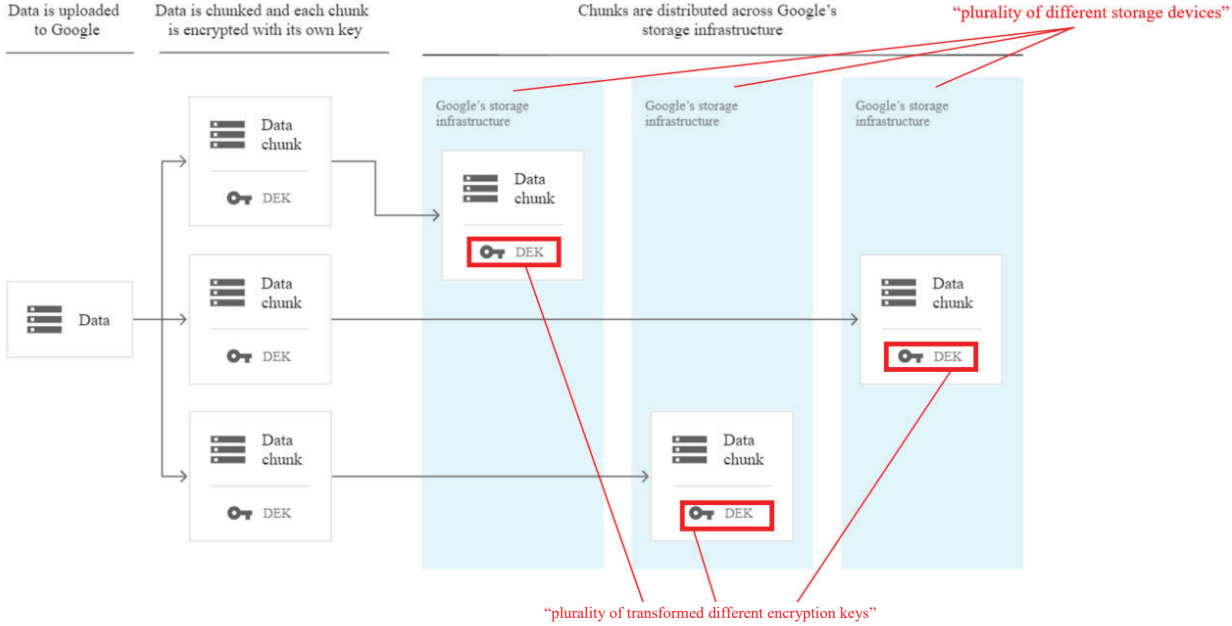
¹⁴ SFI-GOOGLE_000005992.

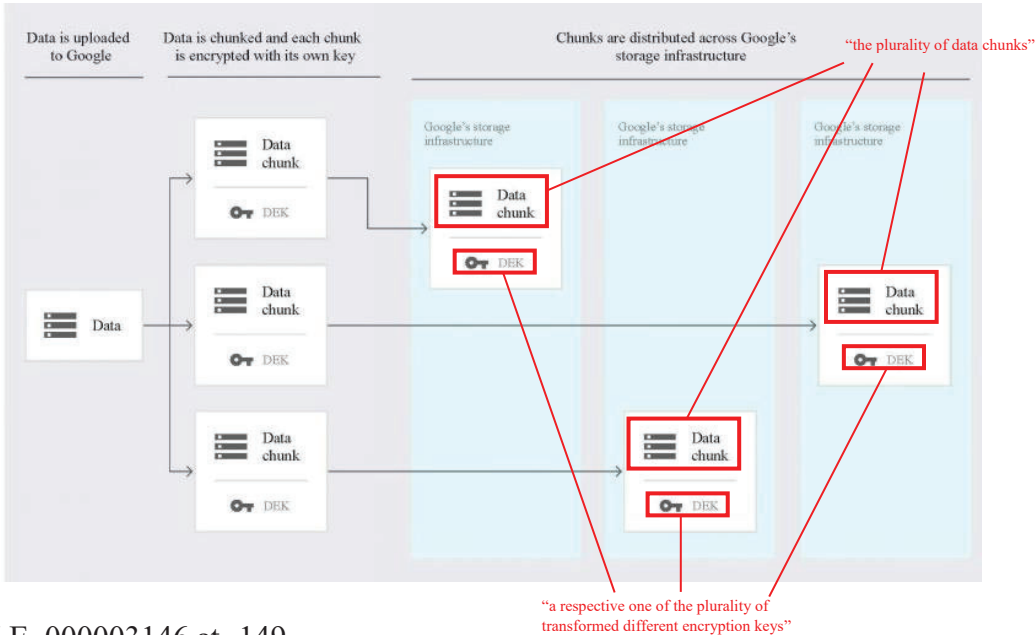
¹⁵ *See also* SFI-GOOGLE_000005933.

¹⁶ SFI-GOOGLE_000005992; *see also* SFI-GOOGLE_000005803 ("Rather than storing each user's data on a single machine or set of machines, we distribute all data . . . across many computers in different locations.").

¹⁷ SFI-GOOGLE_000005816.

¹⁸ SFI-GOOGLE_000005887.

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
	 The diagram illustrates the process of Google's "Encryption at Rest": Data is uploaded to Google: A box labeled "Data" is shown. Data is chunked and each chunk is encrypted with its own key: The data is split into three "Data chunk" boxes, each associated with a unique "DEK" (Data Encryption Key) represented by a key icon. Chunks are distributed across Google's storage infrastructure: The three data chunks and their respective DEKs are distributed across three separate "Google's storage infrastructure" blocks. Annotations: - Red arrows point to the three storage infrastructure blocks with the text: "plurality of different storage devices". - Red boxes highlight the DEKs stored with each data chunk in the infrastructure, with a red arrow pointing to them from the text: "plurality of transformed different encryption keys". SFI-GOOGLE_000003146 at -149.
Claim 11[pre] The method of claim 9,	Google's "Encryption at Rest" comprises the method of claim 9. <i>See</i> Claim 9, <i>supra</i> .
11[a] wherein storing the plurality of data chunks with the plurality of transformed different encryption keys comprises storing each of the plurality of data	Within Google's "Encryption at Rest," storing the plurality of data chunks with the plurality of transformed different encryption keys comprises storing each of the plurality of data chunks with a respective one of the plurality of transformed different encryption keys. For example, each transformed DEK is stored with the data chunk it encrypts. Google explains that "[t]he storage system generates DEKs using Google's common cryptographic library. In general, DEKS are then sent to Keystore to wrap with that storage system's KEK, and the wrapped DEKS are passed back to the storage system to be kept with the data chunks." SFI-GOOGLE_000003146 at -151. Google explains that

U.S. Patent No. 11,178,116	Google's "Encryption at Rest" ¹
chunks with a respective one of the plurality of transformed different encryption keys.	“[b]ecause of the high volume of keys at Google, and the need for low latency and high availability, DEKs are stored near the data that they encrypt.” SFI-GOOGLE_000003146 at -150; <i>see also</i> SFI-GOOGLE_000005743 (Cloud Key Management Service). Below is an exemplary annotated image from the Google Cloud webpage showing how a DEK is stored with its corresponding data chunk:  SFI-GOOGLE_000003146 at -149. As another example, below is an image from Google Cloud's webpage illustrating that every encrypted chunk is stored with its wrapped DEK.¹⁹

¹⁹ SFI-GOOGLE_000005887.

