CHART D – U.S. PATENT NO. 9,338,140

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
Claim 1[pre] A secure storage network comprising[2]	Google's "Encryption at Rest" comprises a secure storage network. Google states its "comprehensive security strategy includes encryption at rest," and that it "encrypt[s] all Google customer content at rest, without any action required by" the customer. SFI-GOOGLE_000003146, *Default encryption at rest*, GOOGLE CLOUD. "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." SFI-GOOGLE_000003146; *see also* SFI-GOOGLE_000005743, *Cloud Key Management Service deep dive*, Google Cloud (last visited Aug. 14, 2023), https://cloud.google.com/docs/security/key-management-deep-dive (Cloud Key Management System). Google securely stores data using "several layers of encryption that are generally used to protect user data in Google production data centers," SFI-GOOGLE_000003146 at -148. Encryption occurs throughout Google's storage system network within those data centers.[3] For example, Google states that "[w]hen you upload a file of any type to Google Drive, it is stored securely in our world-class data centers. Data is encrypted in-transit and at-rest."[4] *See* SFI-GOOGLE_000003287 at -291, *How Google Workspace uses encryption to protect your data* (Aug. 2020) ("In Google's data

[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 with the accused "Encryption at Rest" technology, and on that basis, infringes the '140 Patent in combination with the fact that each Accused Service presents a virtual disk to customers as explained herein.

[2] SFI contends that each element of every asserted claim of the '140 Patent is literally present in each of the Accused Services. To the extent any such element is not literally present, SFI contends such element is present under the doctrine of equivalents.

[3] SFI-GOOGLE_000005933, Google Cloud Tech, *Google Cloud Encryption at Rest*, YOUTUBE (Dec. 12, 2017), https://www.youtube.com/watch?v=Svz2KHE1mdM.

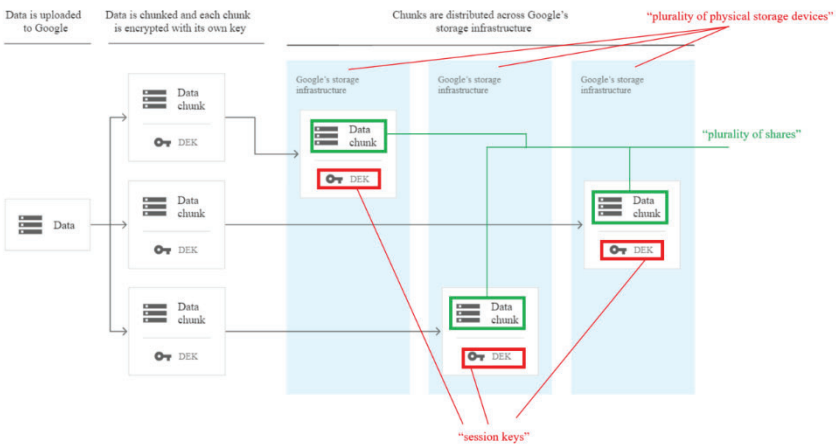
[4] SFI-GOOGLE_000005994, *How Drive Protects Your Privacy & Keeps You in Control*, Google Drive Help, https://support.google.com/drive/answer/10375054?hl=en (last visited Aug. 14, 2023).

Google Exhibit 1037
Google v. SFI

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	centers, data belonging to Google Workspace customers is stored at rest in two types of systems: disks and backup media.").
1[a] a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure a dataset; and	Google's "Encryption at Rest" comprises a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure a dataset. For example, Google splits a user data set into a plurality of shares, each share being associated with a data encryption key ("DEK"), and each share and DEK are stored on one of a plurality of physical storage devices. *See* SFI-GOOGLE_000003146 at -148 ("Data is broken into subfile chunks for storage"); *id*. ("[e]ach chunk is encrypted at the storage level with an individual data encryption key (DEK)"); *id*. ("[e]ach chunk is distributed across our storage systems and is replicated in encrypted form for backup and disaster recovery."). Google Cloud uses symmetric encryption algorithms to secure a dataset, such as AES-GCM (256 bits) protocol, for encryption at rest of data using the session keys, or the DEKs. *See, e.g.*, SFI-GOOGLE_000003146 at -156; *see also* SFI-GOOGLE_000005743 (Cloud Key Management System). Below is an exemplary annotated image from the Google Cloud webpage showing an example of a plurality of physical storage devices, a plurality of shares, and at least one session key used to secure a dataset[5]:

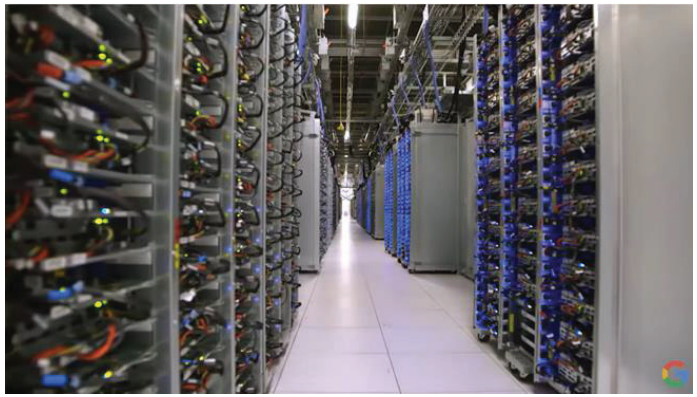
[5] The red and/or green boxes and accompanying text are annotations added by SFC for purposes of this claim chart.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]



SFI-GOOGLE_000003146 at -148.

Below is an exemplary image depicting physical storage devices for, *e.g.*, processing customer data and storing encrypted data and associated keys within a Google data center.



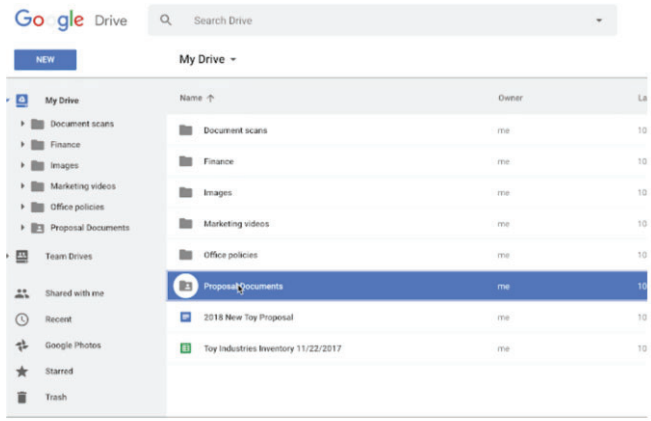
SFI-GOOGLE_000006005, Google Workspace, *Inside a Google data center*, YOUTUBE (Dec. 16, 2014), https://www.youtube.com/watch?v=XZmGGAbHqa0.

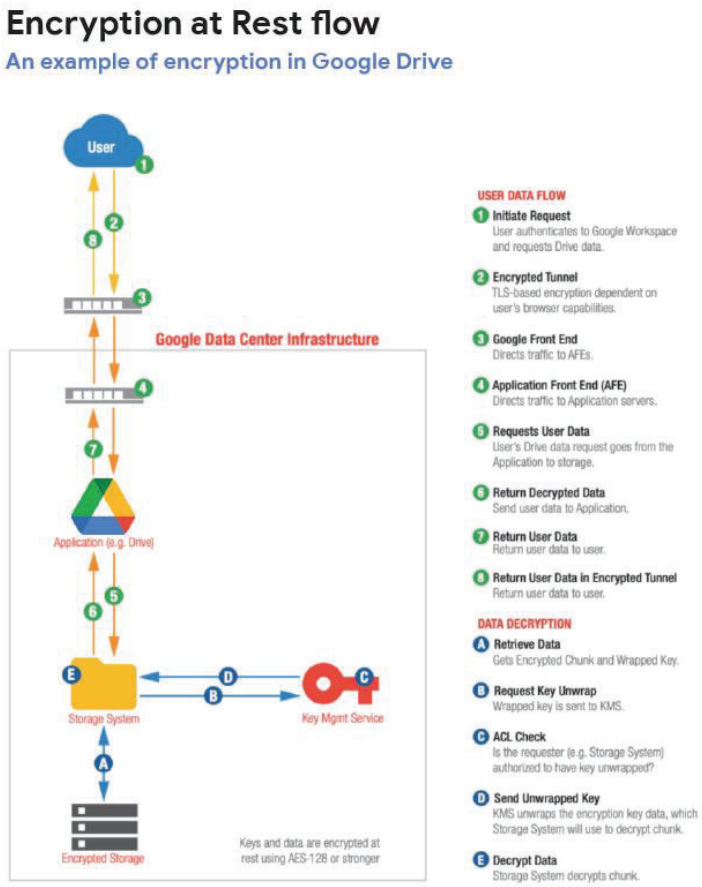
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
1[b] a secure storage system configured to	Google's "Encryption at Rest" comprises a secure storage system. Google states its "comprehensive security strategy includes encryption at rest," and that it "encrypt[s] all Google customer content at rest, without any action required by [the customer], using one or more encryption mechanisms." SFI-GOOGLE_000003146. Google securely stores data using "several layers of encryption that are generally used to protect user data in Google production data centers," SFI-GOOGLE_000003146 at -148. Encryption occurs throughout Google's storage system.[6] For example, Google Drive and Google Cloud comprise secure storage networks. Google states that "[w]hen you upload a file of any type to Google Drive, it is stored securely in our world-class data centers. Data is encrypted in-transit and at-rest."[7] *See* SFI-GOOGLE_000003287 at -291 ("In Google's data centers, data belonging to Google Workspace customers is stored at rest in two types of systems: disks and backup media.").
1[b][i] present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device;	Each of the Accused Services is configured to present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device. According to Google, a virtual disk, in the context of Google's products and services, is "a bunch of pieces from real physical machines spread out over a data warehouse or data center, pulled together, and presented to . . . the user as one logical disk [to] work with and operate on."[8]

[6] SFI-GOOGLE_000005933.

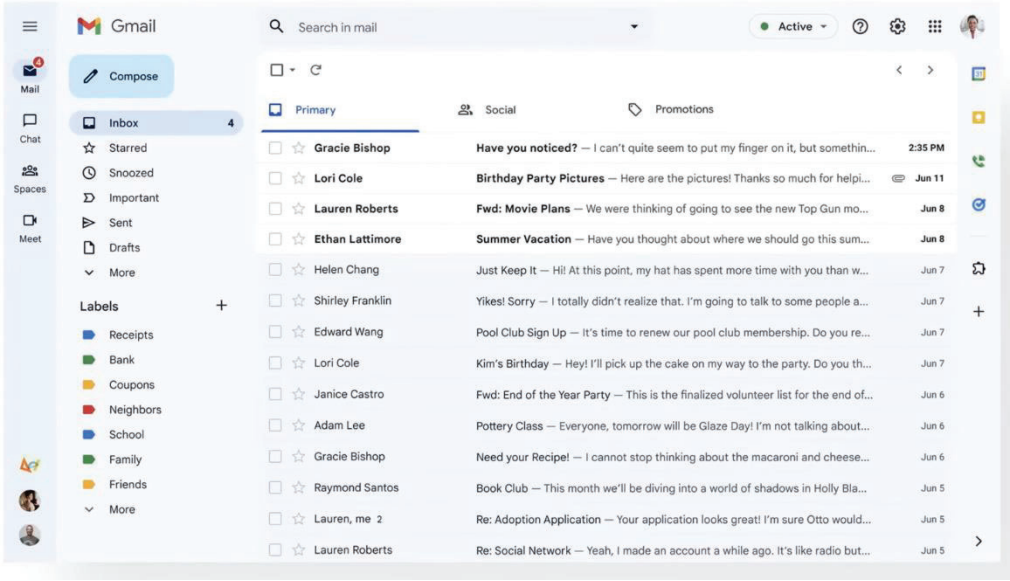
[7] SFI-GOOGLE_000005994.

[8] SFI-GOOGLE_000006048, Google Cloud Tech, *What is a disk in Cloud VM?*, YOUTUBE (Sep. 25, 2021), https://www.youtube.com/watch?v=QySbgQIcOvk.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Accused Google Services Google Drive For example, Google presents a virtual disk to a client device through Google Drive. *See, e.g.*, *Search Within a Folder in Google Drive, Google Workspace Updates* (Jan. 9, 2018) https://workspaceupdates.googleblog.com/2018/01/search-within-folder-in-google-drive.html:  The virtual disk comprises a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device at least because, for example, the Google Drive directory shows files which are stored, on a plurality of physical storage devices, using Google Cloud encryption technology, but does not show the location of those storage devices. *See* SFI-GOOGLE_000003287 at -295.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	 Gmail Gmail presents to the client a virtual disk. The virtual disk comprises a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device at least because, for example, the Gmail inbox displays a directory that shows files, such as emails and attachments,

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	which are stored on a plurality of physical storage devices, using Google Cloud encryption technology, but does not show the location of those storage devices.[9]

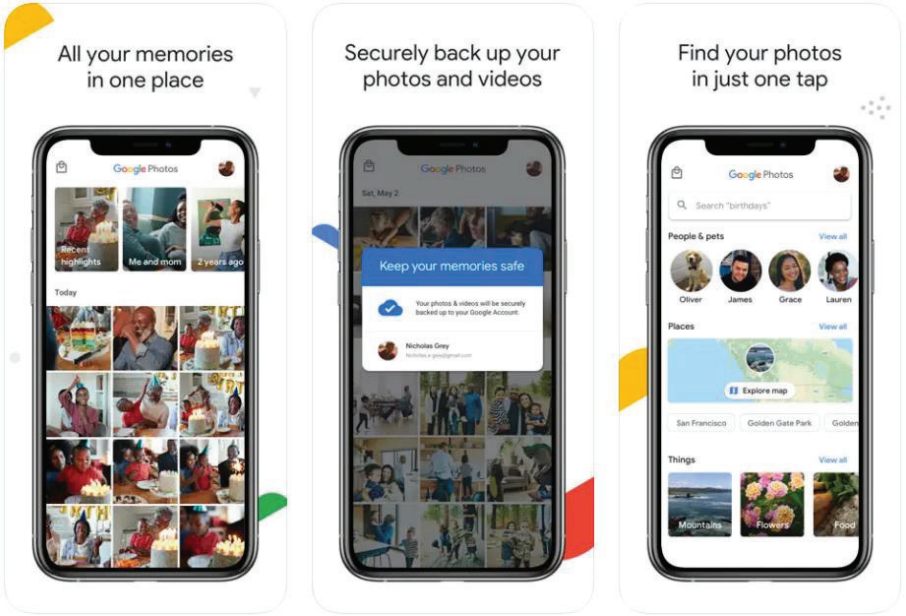


Google Photos

Google Photos presents to the client a virtual disk. The virtual disk comprises a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device at least because, for example, the Google Photos directory shows files which are stored, on a plurality of physical storage devices, using Google Cloud encryption technology, but does not show the location of those storage devices.[10]

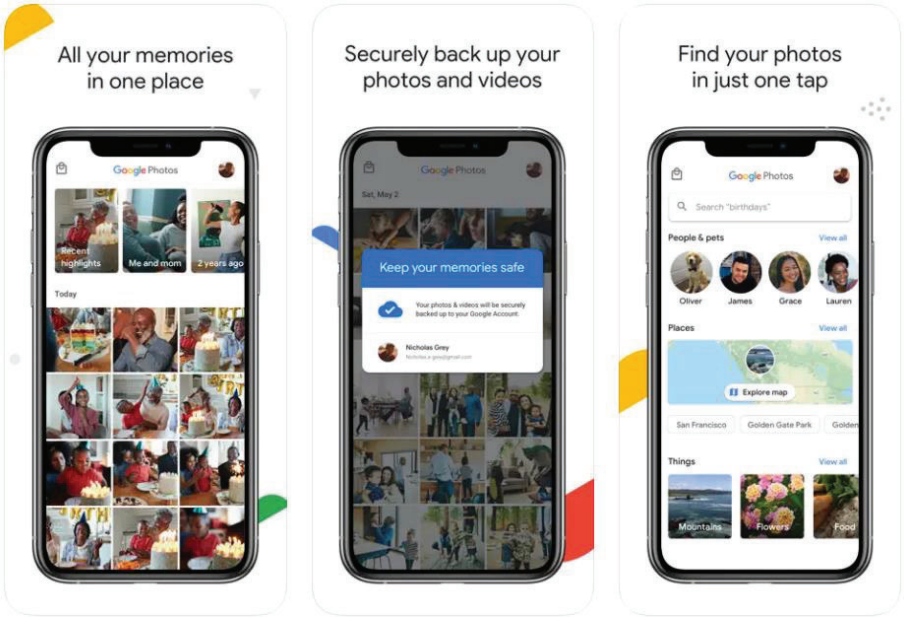
[9] Google Workspace, *The Evolution of Gmail*, YOUTUBE (July 28, 2022), https://www.youtube.com/watch?v=AbuQ3rXgrfg.

[10] *Google Photos*, APPLE: APP STORE (last visited Aug. 14, 2023), https://apps.apple.com/us/app/google-photos/id962194608?platform=messages.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	 * * * **Accused Google Cloud Services** Google Workspace Google Workspace presents to the client device a virtual disk, including for Google Photos, among several other features within Workspace.[11] The virtual disk comprises a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device at least because, for example, the Google Photos directory shows files which are stored, on a plurality of physical

[11] *See, e.g.*, *Google Photos*, GOOGLE (last visited Aug. 14, 2023), https://www.google.com/photos/about/.

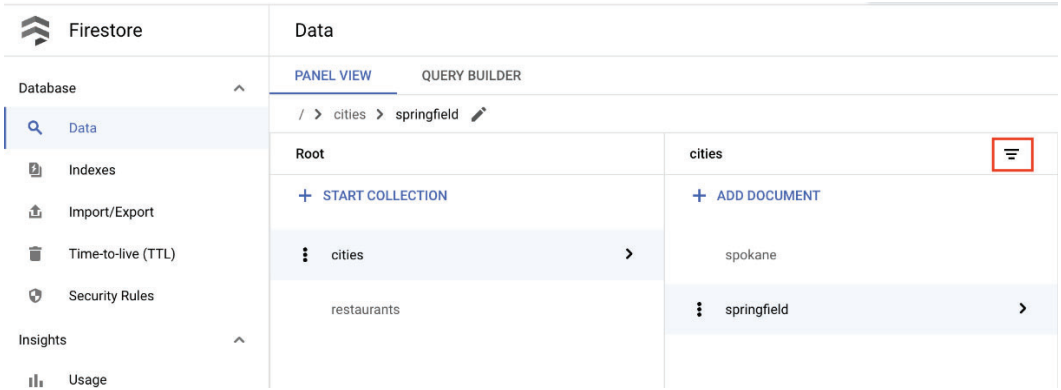
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	storage devices, using Google Cloud encryption technology, but does not show the location of those storage devices.[12]



Google Cloud Platform

As explained in the body of SFI's response to Google's Interrogatory No. 7, several specific products and services within Google Cloud Platform store customer data with "Encryption at Rest." The following exemplary images show presentation by each such product or service of a virtual disk to the client, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device. This is done by, for example, allowing a developer

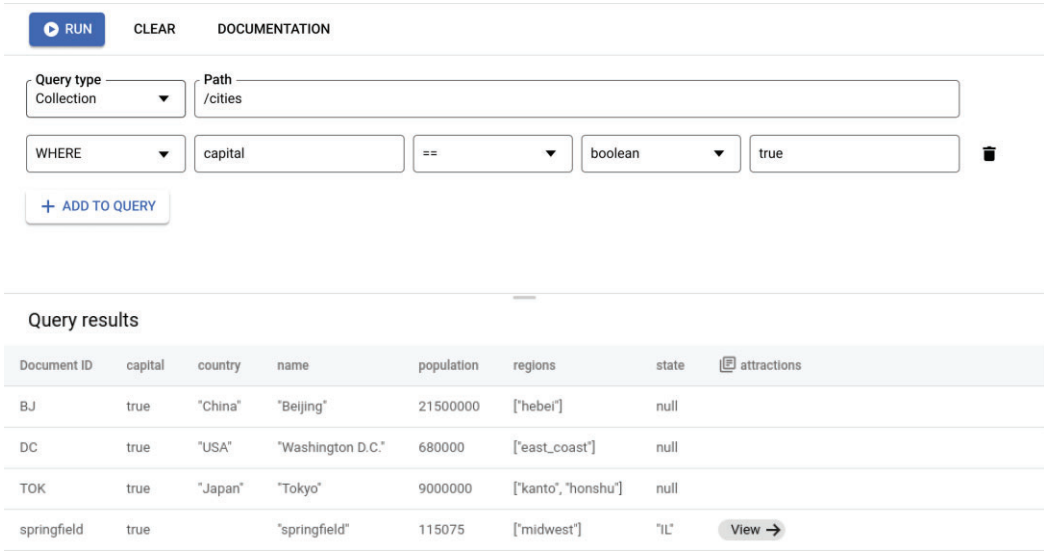
[12] *Google Photos*, APPLE: APP STORE (last visited Aug. 14, 2023), https://apps.apple.com/us/app/google-photos/id962194608?platform=messages.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	to view and organize data specific to each product that is stored on a plurality of physical storage devices, using Google Cloud encryption technology, but without showing the location of those storage devices. *Firestore* Google Cloud Firestore stores non-relational data and presents to developers via the Google Cloud Console a directory where a user can "view data" by "click[ing] on a document or collection to open the data nested within that item."[13] Below are images depicting the virtual disk and directory presented to a Firestore user's device. This virtual disk allows a user to interact with data that is stored on physical storage devices without revealing the physical location of the data[14,15]: 

[13] SFI-GOOGLE_000006009, *Managing Firestore with the console*, GOOGLE CLOUD (last updated Aug. 8, 2023), https://cloud.google.com/firestore/docs/using-console.

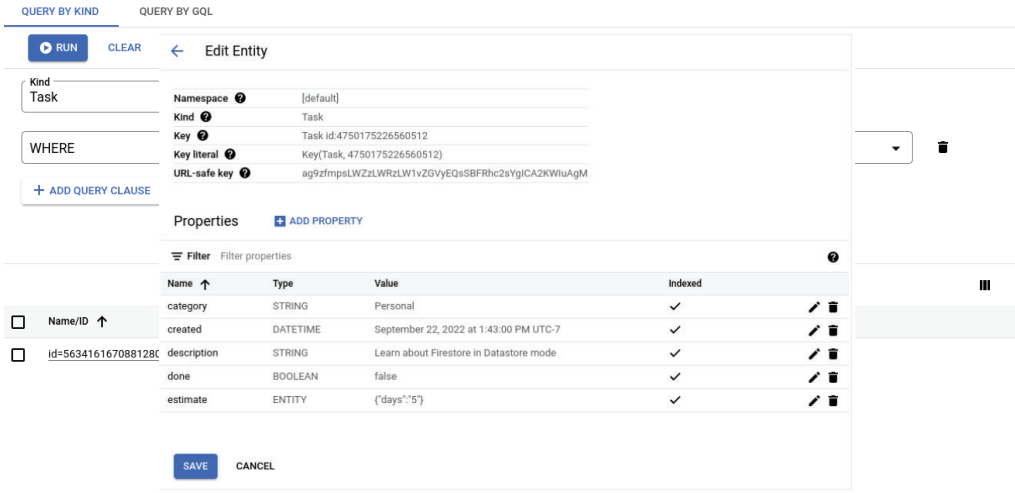
[14] SFI-GOOGLE_000006009.

[15] SFI-GOOGLE_000006009.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	 *Firestore in Datastore Mode*[16] Google Cloud Firestore in Datastore mode stores non-relational data and presents to developers via the Google Cloud Console a directory where a user can, for example, create databases and run queries on these databases.[17]

[16] SFI understands that Firestore is a subsequent generation of Datastore, and is able to store and query data in "Firestore in Datastore" mode. *See* SFI-GOOGLE_000005829, *Datastore*, GOOGLE CLOUD (last visited Aug. 14, 2023), https://cloud.google.com/datastore; SFI-GOOGLE_000006034, *Store and query data in Firestore in Datastore mode*, GOOGLE CLOUD (last updated Aug. 7, 2023), https://cloud.google.com/datastore/docs/store-query-data.

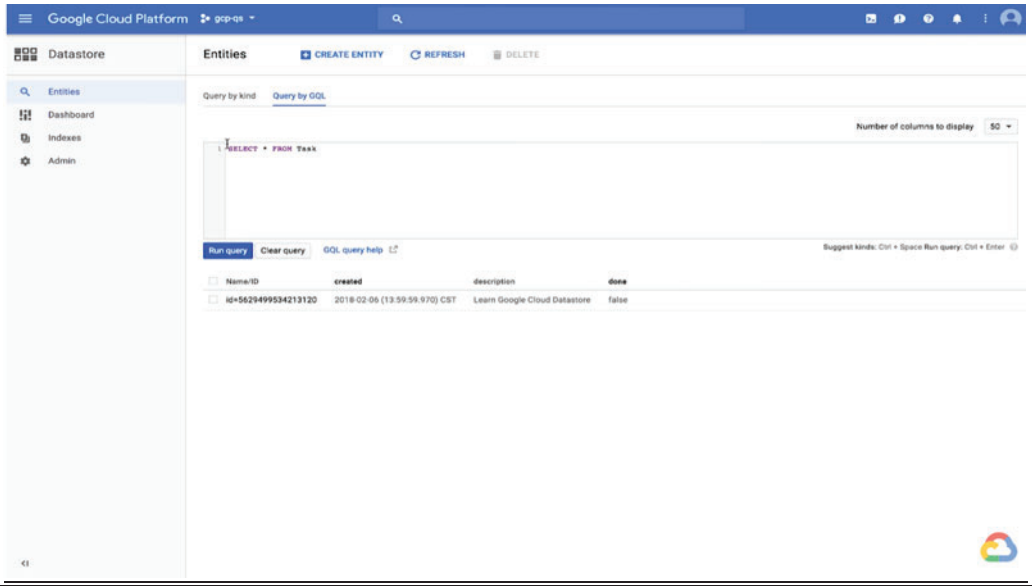
[17] SFI-GOOGLE_000006009.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Below are exemplary images depicting the virtual disk and directory presented to a Firestore user's device.[18] This virtual disk allows a user to interact with data that is stored on physical storage devices without revealing the physical location of the data.[19]  *Datastore*[20] Datastore stores non-relational data and presents to developers via the Google Cloud Console a directory where a user can navigate stored data on a virtual disk.

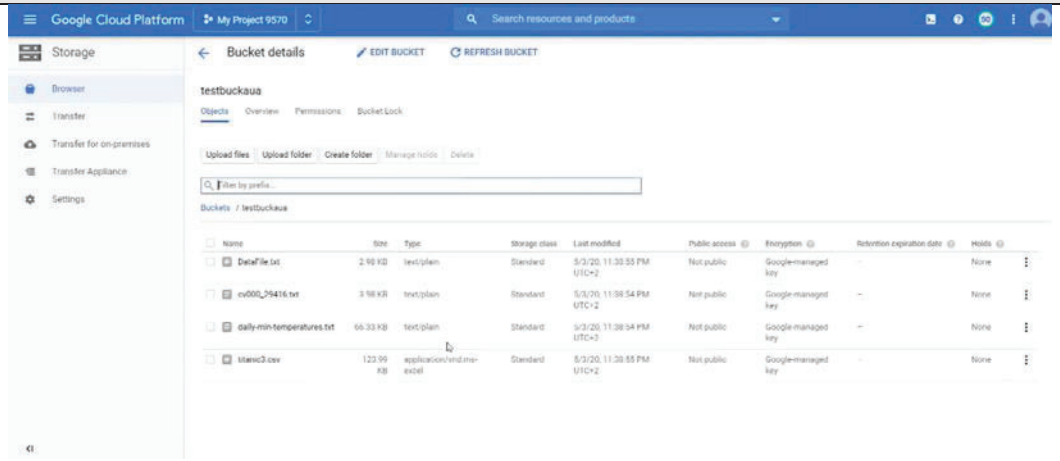
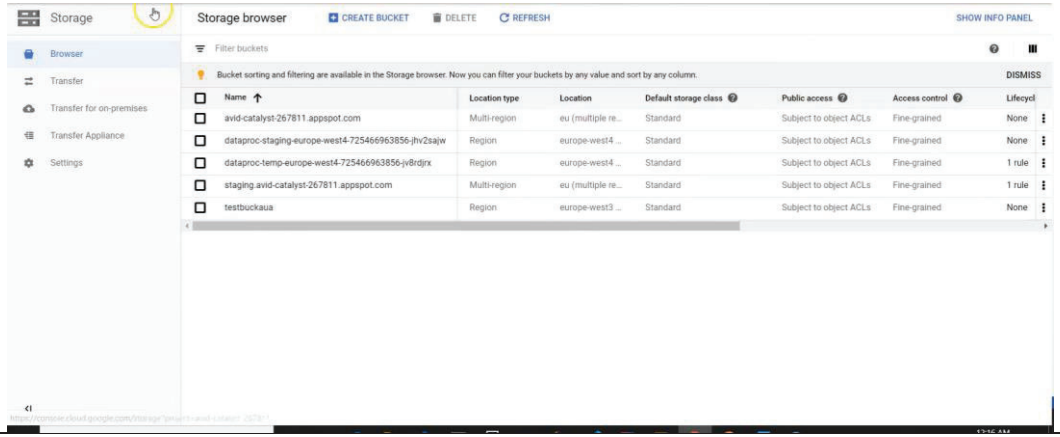
[18] SFI-GOOGLE_000006034.

[19] SFI-GOOGLE_000006034.

[20] Although SFI understands that Datastore is no longer used natively and all existing Datastore users have been upgraded to Firestore or Firestore in Datastore mode, SFI also understands that Datastore used default encryption at rest and was used by customers during a relevant period. SFI-GOOGLE_000005829.

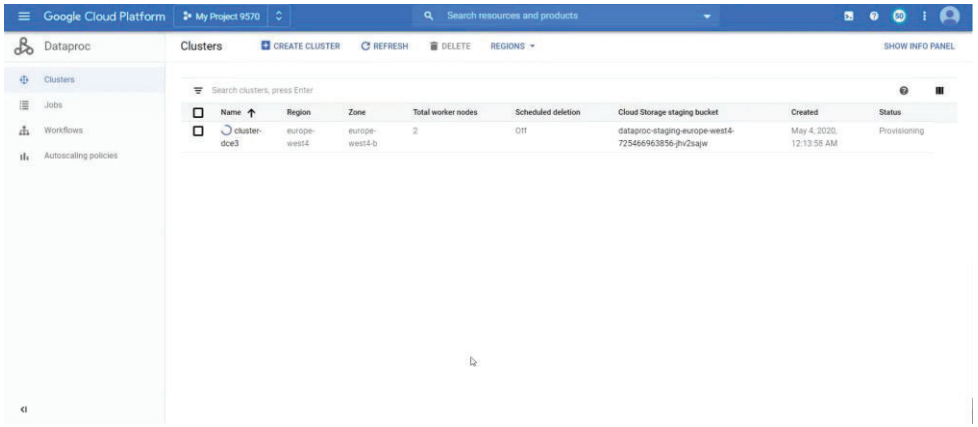
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Below are exemplary images depicting the virtual disk and directory presented to a Datastore user's device. This virtual disk allows a user to interact with data, called "entities," that is stored on physical storage devices without revealing the physical location of the data[21]: 

[21] SFI-GOOGLE_000005827, Google Cloud Tech, *Datastore*, YOUTUBE (June 12, 2018), https://www.youtube.com/watch?v=oDQlSrMyHL0.

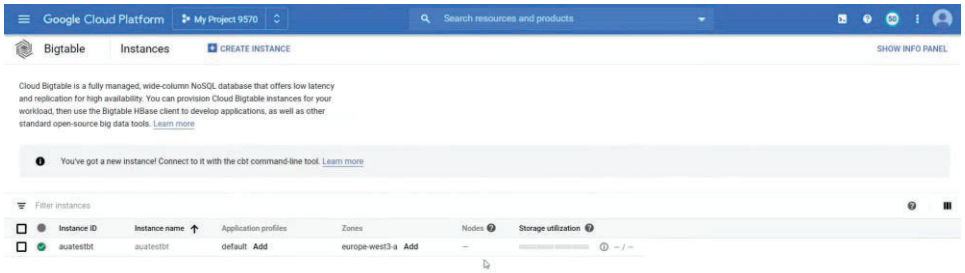
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	 *Cloud Storage*[22] 

[22] SFI-GOOGLE_000005935, Simplilearn, *Google Cloud Platform Tutorial | GCP Tutorial | Google Cloud Platform For Beginners | Simplilearn*, YOUTUBE (May 13, 2020), https://www.youtube.com/watch?v=vACTtmLWiQY.

Data Proc[23]

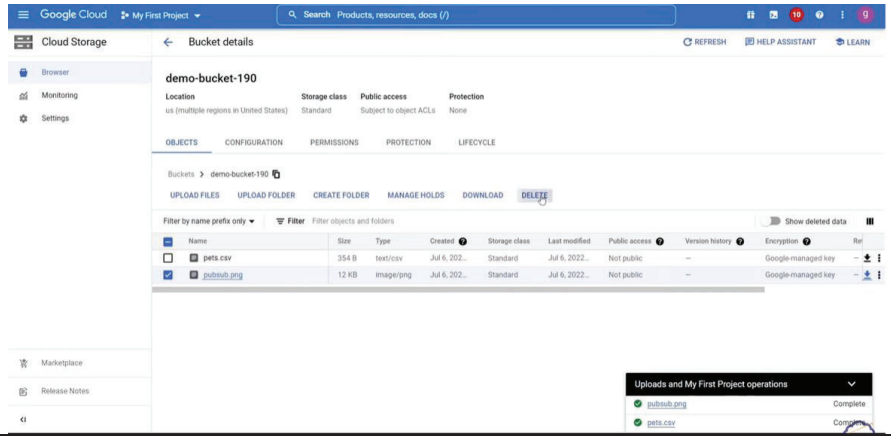


Bigtable[24]

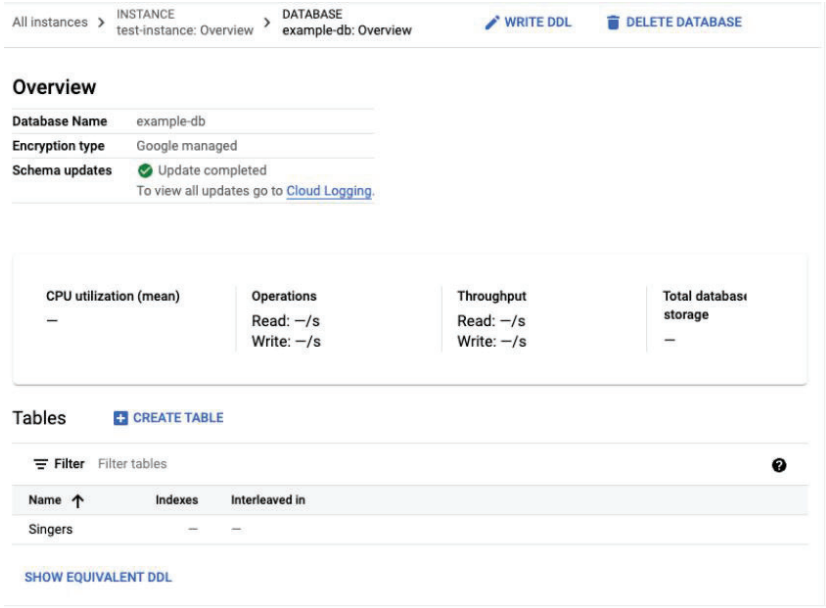


[23] SFI-GOOGLE_000005935.

[24] SFI-GOOGLE_000005935.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Pub/sub[25] 

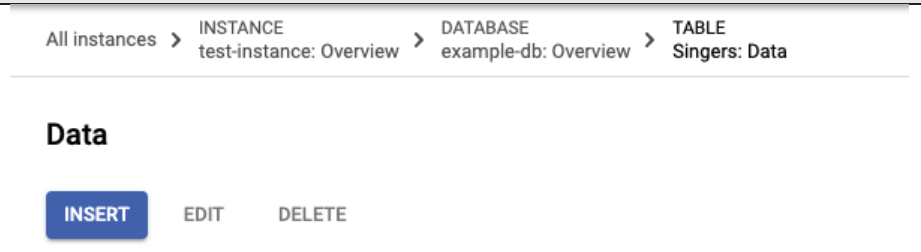
[25] SFI-GOOGLE_000005940, SkillCurb, *Google Cloud PubSub beginners hands on Lab*, YOUTUBE (July 21, 2011), https://www.youtube.com/watch?v=jYIgcdIW1yk.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Cloud Spanner[26,27] 

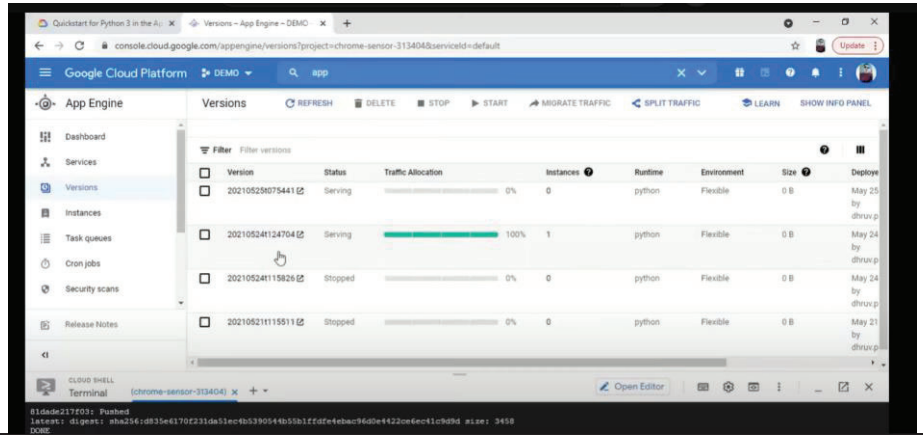
[26] SFI-GOOGLE_000005782, *Create and query a database by using the Google Cloud console*, GOOGLE CLOUD (last updated Aug. 4, 2023) https://cloud.google.com/spanner/docs/create-query-database-console.

[27] SFI-GOOGLE_000005782.

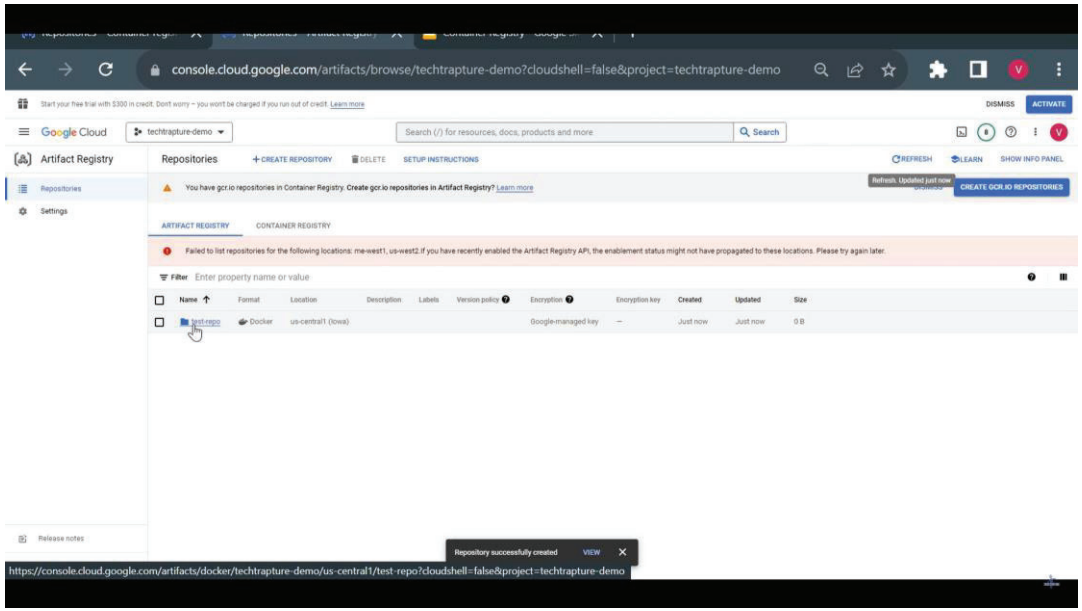
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]



App Engine[28]

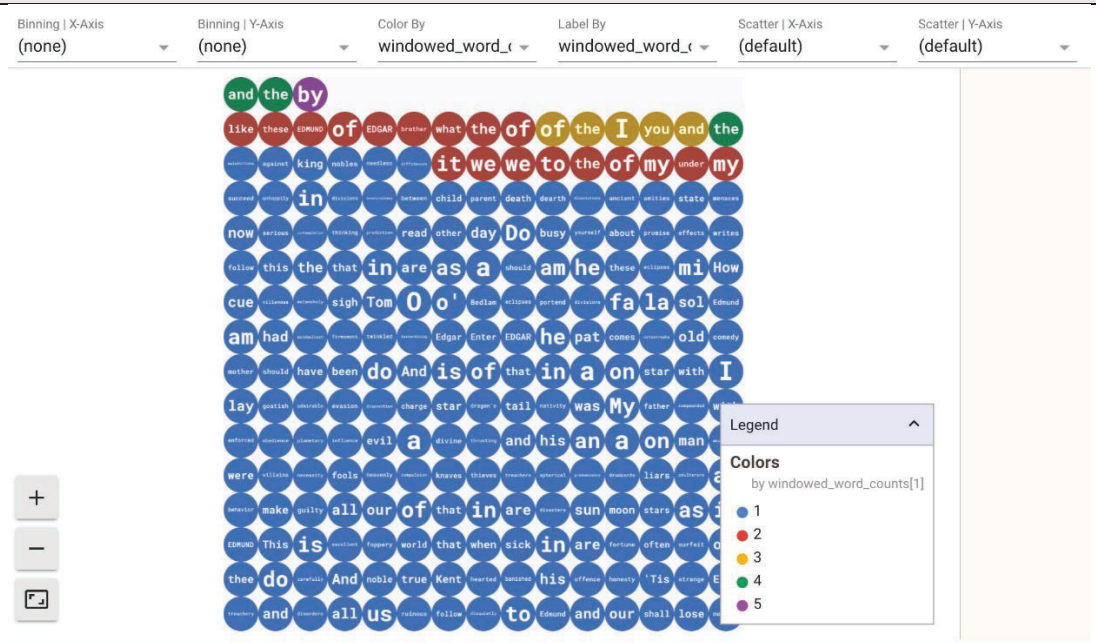


[28] SFI-GOOGLE_000005929, edureka!, *Google Cloud App Engine | Google App Engine Tutorial | Google Cloud Platform Training | Edureka*, YOUTUBE (May 27, 2021), https://www.youtube.com/watch?v=SKlZzLctmGc.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Artifact Registry[29,30] 

[29] SFI-GOOGLE_000005858, TechTrapture, *difference between container registry and artifact registry*, YOUTUBE (Jan. 22, 2023), https://www.youtube.com/watch?v=mz32F3R0AkU.

[30] SFI-GOOGLE_000005836, *Develop Apache Beam notebooks with the interactive runner*, GOOGLE CLOUD: DATAFLOW (last visited Aug. 14, 2023), https://cloud.google.com/dataflow/docs/guides/interactive-pipeline-development#read_and_visualize_the_data.

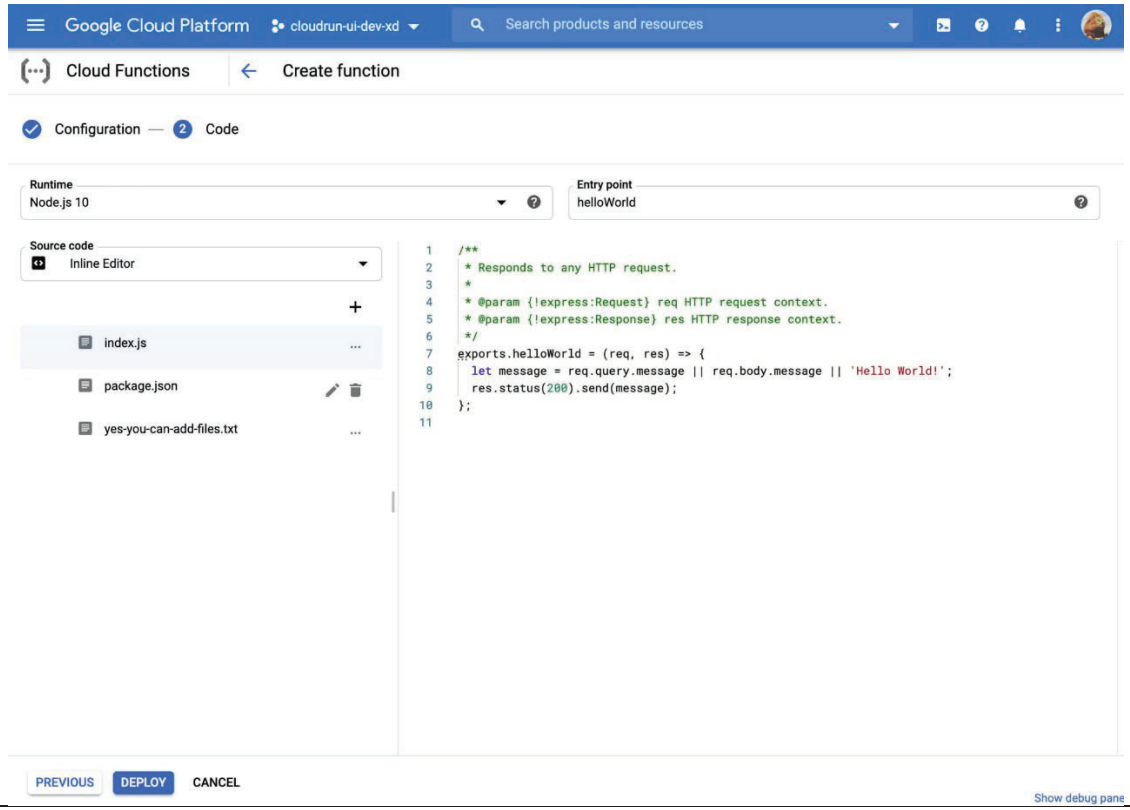
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	

Dataflow[31]

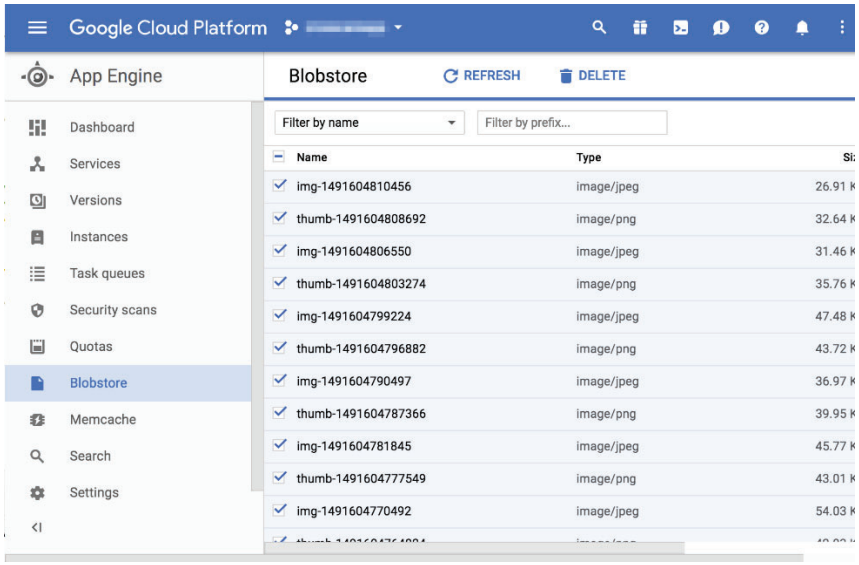
```
ib.collect(windowed_lower_word_counts, include_window_info=True, n=20, duration=30)
```

	0	1	event_time	windows	pane_info
0	b'this'	1	1621363389999999	[[1621363380.0, 1621363390.0)]	PaneInfo(first: True, last: False, timing: ON_...
1	b'not'	1	1621363389999999	[[1621363380.0, 1621363390.0)]	PaneInfo(first: True, last: False, timing: ON_...
2	b'is'	1	1621363389999999	[[1621363380.0, 1621363390.0)]	PaneInfo(first: True, last: False, timing: ON_...
3	b'lear'	1	1621363389999999	[[1621363380.0, 1621363390.0)]	PaneInfo(first: True, last: False, timing: ON_...
4	b'doth'	1	1621363389999999	[[1621363380.0, 1621363390.0)]	PaneInfo(first: True, last: False, timing: ON_...
5	b'not'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
6	b'is'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
7	b'lear'	2	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
8	b'walk'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
9	b'where'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
10	b'thus'	2	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
11	b'are'	2	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
12	b'speak'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
13	b'his'	3	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
14	b'eyes'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
15	b'either'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
16	b'notion'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
17	b'weakens'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
18	b'discernings'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...
19	b'waking'	1	1621363399999999	[[1621363390.0, 1621363400.0)]	PaneInfo(first: True, last: False, timing: ON_...

[31] SFI-GOOGLE_000005836.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Cloud Functions[32] 

[32] SFI-GOOGLE_000005726, Dustin Ingram & Vinod Ramachandran, *New in Cloud Functions: languages, availability, portability, and more*, GOOGLE CLOUD: BLOG (Oct. 5, 2020), https://cloud.google.com/blog/products/serverless/a-roundup-of-cloud-functions-enhancements.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	App Engine[33]  * * * **Fitbit** Fitbit by Google wearable devices and the Fitbit app present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device.

[33] SFI-GOOGLE_000005899, Jason More, *Download all files in Google App Engine Blobstore*, STACK OVERFLOW: BLOG (Aug. 4, 2017), https://stackoverflow.com/questions/45511598/download-all-files-in-google-app-engine-blobstore.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	As an example, when a user creates a new Fitbit account using their Google Account,[34] data collected from Fitbit devices is stored and secured on Google's servers.[35] Users of Fitbit devices or the Fitbit app can view and interact with health and personal data that is stored on Google's servers without knowing the physical locations of their data. Below is an exemplary image of a Fitbit user dashboard showing a user's data that is stored on Google's servers.[36] Below are images depicting a Fitbit device display with user data collected that is stored on Google's servers.[37]

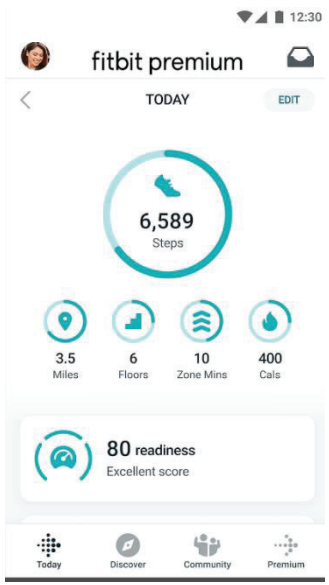
[34] SFI understands that new Fitbit users are required to register with their Google account, and existing Fitbit users have the option to move their Fitbit account to a Google account. All Fitbit users will be required to move to a Google account in 2025. *See* SFI-GOOGLE_000006050, *What should I know about moving Fitbit to my Google Account?*, FITBIT HELP (last visited Aug. 14, 2023), https://help.fitbit.com/articles/en_US/Help_article/2478.htm; SFI-GOOGLE_000005901, *FAQs on Privacy: Fitbit*, GOOGLE SUPPORT: PRODUCT DOCUMENTATION HELP (last updated July 3, 2023), https://support.google.com/product-documentation/answer/13532616?sjid=16648661610313590450-NA.

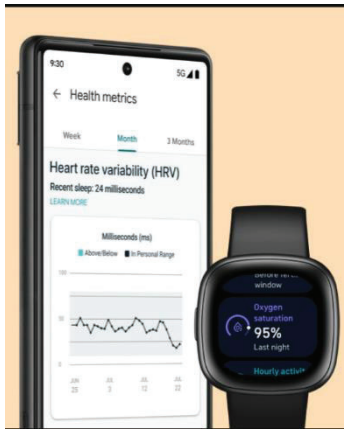
[35] SFI-GOOGLE_000005901.

[36] SFI-GOOGLE_000005909, Fitbit LLC, *Fitbit*, GOOGLE PLAY (last visited Aug. 14, 2023), https://play.google.com/store/apps/details?id=com.fitbit.FitbitMobile&hl=en_US&gl=US.

[37] SFI-GOOGLE_000006043, *versa 4*, FITBIT (last visited Aug. 14, 2023) https://www.fitbit.com/global/us/products/smartwatches/versa4?sku=523BKBK.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]

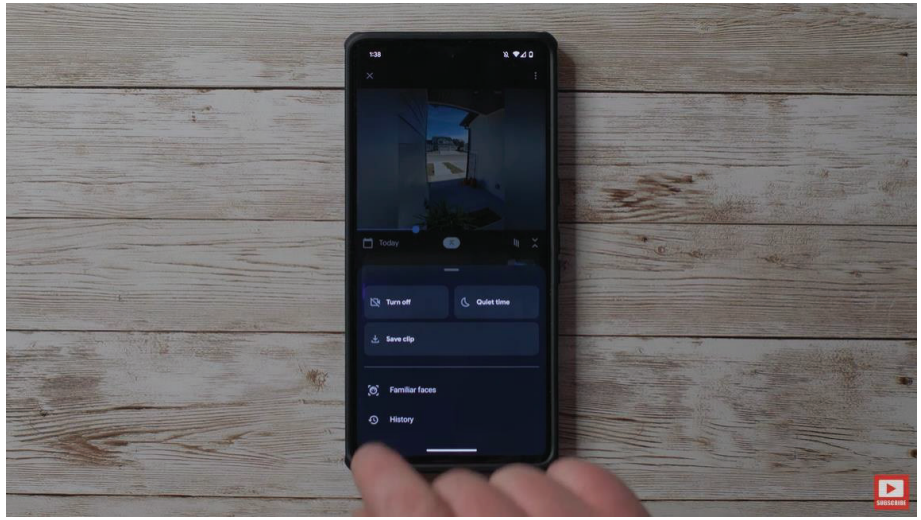




Google Home

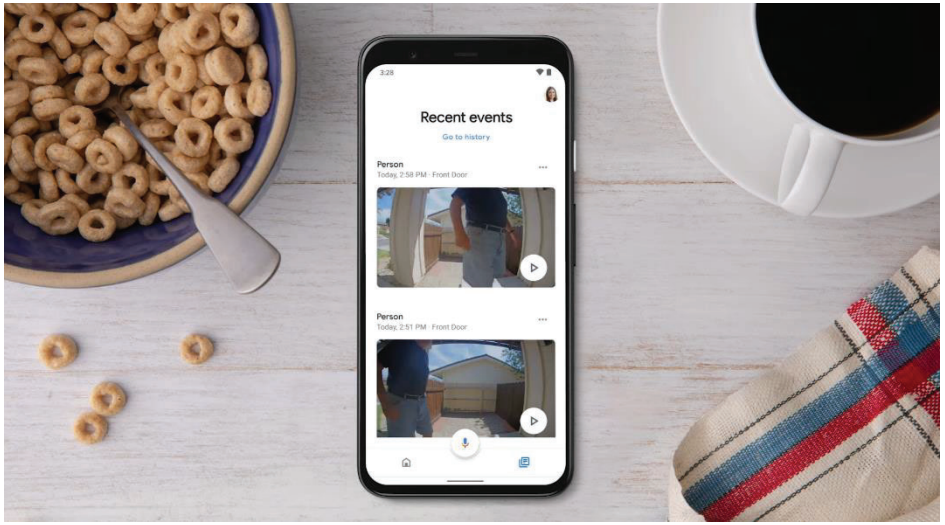
The Google Home App presents to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device. As an example the Google Home App allows users to access data collected from various Google Home devices and services that use Google Accounts; this data is encrypted and stored by Google in its data centers.[38] Users of the Google Home app can access, view, and save videos captured by,

[38] *See, e.g.*, SFI-GOOGLE_000005942, *Nest*, GOOGLE SAFETY CENTER (last visited Aug. 14, 2023), https://safety.google/nest/?utm_source=google-home-rhea&utm_medium=referral&utm_content=what-is-google-home_safer; SFI-GOOGLE_000005813, *Data security and privacy on devices that work with Assistant*, GOOGLE NEST HELP (last visited Aug. 14, 2023), https://support.google.com/googlenest/answer/7072285?hl=en&ref_topic=7173611&sjid=18344368013238314148-NA#zippy=%2Cwhere-are-you-saving-my-data.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	for example, a linked Google Nest device that are stored on Google Cloud. Below is an exemplary image of this feature[39]:  **Google Nest** The Google Nest app presents to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device. As an example, Google Nest products such as the Nest Mini, Nest Hub, or Nest Cam record and store audio, video and photo snapshots that are stored on Google servers in Google data centers via Google Cloud.[40]

[39] SFI-GOOGLE_000005722, Tech with Brett, *2022 Google Home App Public Preview First Look!*, YOUTUBE (Nov. 21, 2022), https://www.youtube.com/watch?v=tL54c0jcq1I.

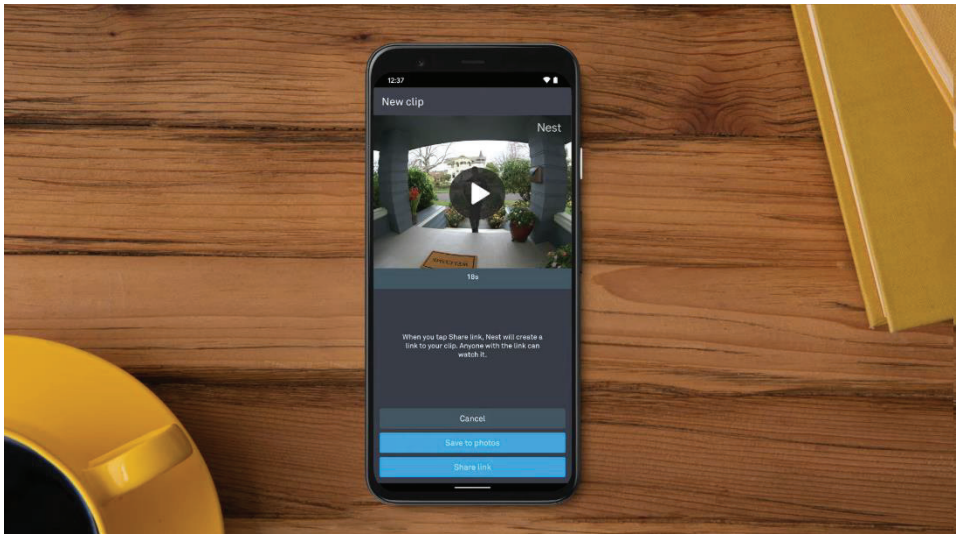
[40] SFI-GOOGLE_000005999, *How Nest cameras store recorded video*, GOOGLE NEST HELP (last visited Aug. 14, 2023), https://support.google.com/googlenest/answer/9242083?sjid=16648661610313590450-NA ("All Google Nest cameras and doorbells can upload and

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Google Nest customers can view data such as video clips or event history collected from a Google Nest product via the Nest app.[41] Below is an exemplary image depicting Recent events and corresponding videos in the Nest app.[42] 

securely save video in the cloud, where it's protected from theft and damage."); SFI-GOOGLE_000005771, *Powering Nest's Camera Cloud with Cloud Spanner*, GOOGLE CLOUD: DATABASES (Mar. 10, 2022), https://cloud.google.com/blog/products/databases/cloud-spanner-is-the-database-of-choice-for-nest-cameras/; SFI-GOOGLE_000005893, *Event and 24/7 video history*, GOOGLE NEST HELP (last visited Aug. 14, 2023), https://support.google.com/googlenest/answer/9681538; SFI-GOOGLE_000005813; SFI-GOOGLE_000006028, Google, *Privacy On Google Assistant*, YOUTUBE (Jan. 7, 2020), https://www.youtube.com/watch?v=ZaqZcDOoi-8.

[41] SFI-GOOGLE_000006041, *Save and download video clips*, GOOGLE NEST HELP (last visited Aug. 14, 2023), https://support.google.com/googlenest/answer/9207572?hl=en&ref_topic=9305896&sjid=16648661610313590450-NA.

[42] SFI-GOOGLE_000006001, Google Nest, *How to see your saved video and event history*, YOUTUBE (June 19, 2020) https://www.youtube.com/watch?v=R0c7kGGbIxs&t=8s.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Within this same Nest app, a customer can save or share a link to video captured on a Nest camera. Below is an exemplary image of this feature.[43]  As another example, Google Nest customers can view a directory of photos stored on Google Cloud servers via the Google Nest Hub. Below is an exemplary image of this feature.[44]

[43] SFI-GOOGLE_000006001; *see also* SFI-GOOGLE_000006041.

[44] SFI-GOOGLE_000005897, Steve DOES, *EVERYTHING You Can Do With The Google Nest Hub*, YOUTUBE (Aug. 17, 2020), https://www.youtube.com/watch?v=AsAeolIKtqQ.

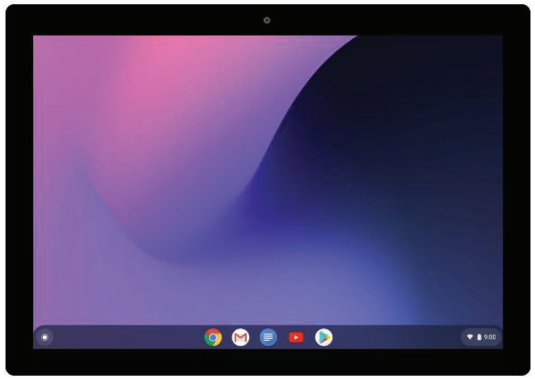
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	 **<u>Chromebook</u>** Google Chromebooks utilize ChromeOS, which contains a desktop version of Google Drive.[45] For example, a user of a Chromebook can view files saved in Google Cloud from the ChromeOS desktop.[46] Below are exemplary images displaying how a Chromebook desktop using ChromeOS presents to the client's device a virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device[47]:

[45] *See, e.g.*, SFI-GOOGLE_000006030, *Questions about Chromebook?*, CHROMEBOOK (last visited Aug. 14, 2023), https://www.google.com/chromebook/switch-qa/#storagedata ("[O]n your local drive on the cloud, you can get the storage you need on a Chromebook.").

[46] *See, e.g.*, *Find and open your files*, CHROMEBOOK SIMULATOR (last visited Aug. 14, 2023), https://partnerdash.google.com/apps/simulator/chromebook.

[47] *Id.*

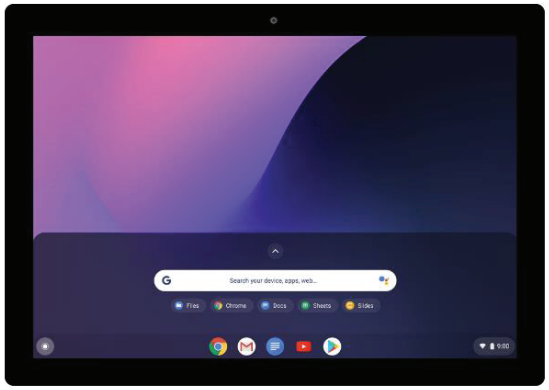
Find and open your files



Step 1 of 5

In the corner of your screen, select the Launcher .

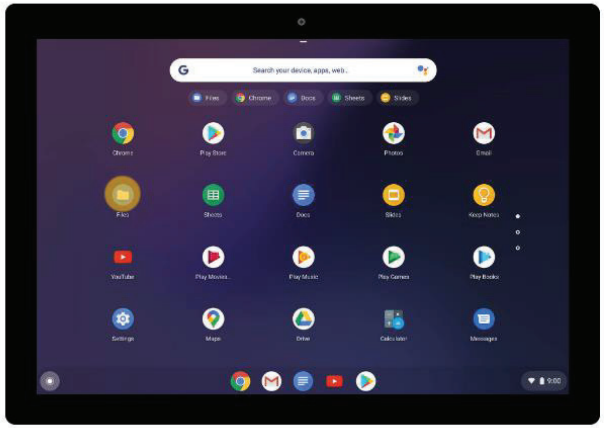
Find and open your files



Step 2 of 5

Select the Up arrow .

Find and open your files

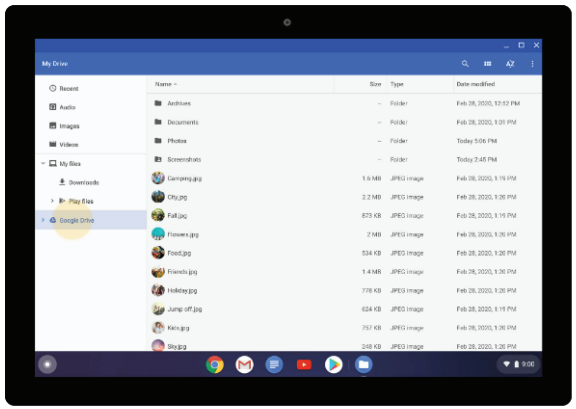


Step 3 of 5

Open Files .

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]

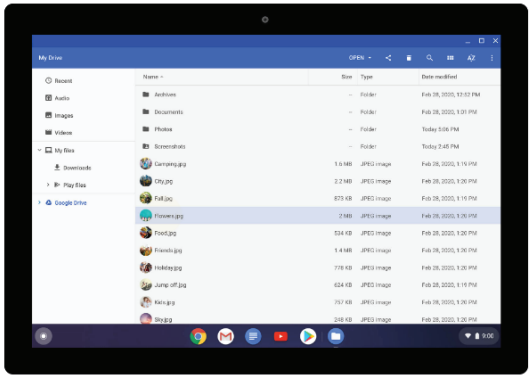
Find and open your files



Step 4 of 5

On the left, choose a file category, like Recent, Downloads or Google Drive.

Find and open your files



Step 5 of 5

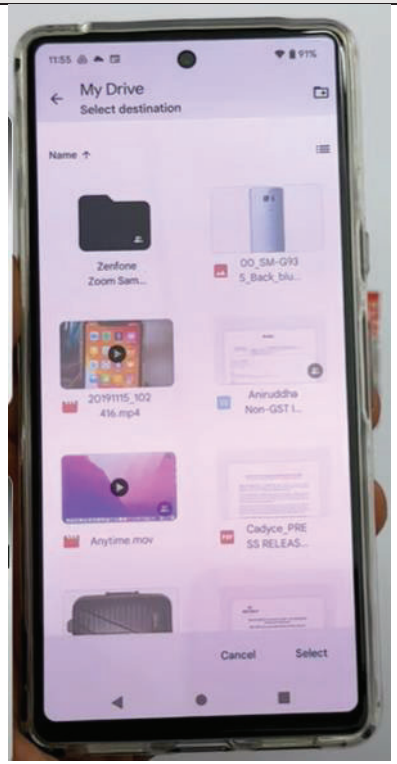
Double-click or tap the file you'd like to open.

Google Pixel

Numerous Google Pixel devices utilize Android and ChromeOS, in which there are application versions of Google Drive.[48] For example, a user of a Pixel 7 can view files saved in Google Cloud from the Android desktop. Below is an exemplary image displaying how a Pixel 7 using Android presents to the client's device a virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device[49]:

[48] *See, e.g.*, SFI-GOOGLE_000006003, *How to use Google Drive*, Google Drive Help, https://support.google.com/drive/answer/2424384 (last visited Aug. 14, 2023).

[49] SFI-GOOGLE_000005987, Tech2touch, *Google Pixel 7/Pixel 7 Pro: How to scan document and make it pdf*, YouTube (Dec. 9, 2022), https://www.youtube.com/watch?v=nISTDQ6-db8.

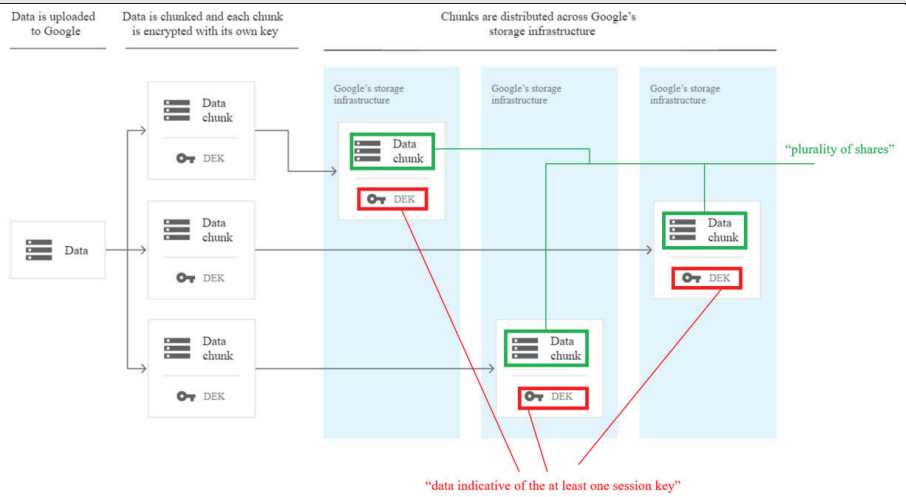
U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	
1[b][ii] generate the plurality of shares for storage on the plurality of physical storage devices by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares;	Google's "Encryption at Rest" comprises a secure storage system configured to generate the plurality of shares for storage on the plurality of physical storage devices by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares. For example, Google generates the plurality of shares for storage on the plurality of physical storage devices by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares through its DEK/KEK system. For example, Google explains that "[e]ach chunk is encrypted at the storage level with an individual data encryption key (DEK)." SFI-GOOGLE_000003146 at -148; *see also id*. ("Google encrypts data before it is written to a database storage system or hardware disk. Encryption is inherent in all of our storage systems, rather than added afterward."). Google explains that "[t]he storage

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	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." *Id*. at -151; *see also* SFI-GOOGLE_000005743 (Cloud Key Management System). Below is an exemplary image from the Google Cloud webpage showing how data is "chunked" and "encrypted":  SFI-GOOGLE_000003146 at -149.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	Google also performs a securing operation on the dataset when, for example, it randomly names the data shares so the shares' names are "unreadable to the human eye," "as an extra measure of security."[50] The dataset is distributed in the shares when, for example, the dataset is broken up into shares for storage. Google states that "[d]ata is broken into subfile chunks for storage." SFI-GOOGLE_000003146 at -148. A dataset uploaded by a Google user, for example, "will not be stored entirely in a single server, but instead will be broken up into chunks" and stored across different servers.[51]
1[b][iii] include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset; and	Google's "Encryption at Rest" comprises a secure storage system configured to include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset. For example, Google stores with the shares data indicative of the at least one session key at least by virtue of storing DEKs with the data shares. *See supra* at Claim 1[a]. Below is an exemplary annotated image from the Google Cloud webpage showing an example of the plurality of shares and data indicative of the at least one session key:

[50] SFI-GOOGLE_000005803, *Data and Security*, GOOGLE DATA CENTERS (last visited Aug. 14, 2023), https://www.google.com/about/datacenters/data-security/.

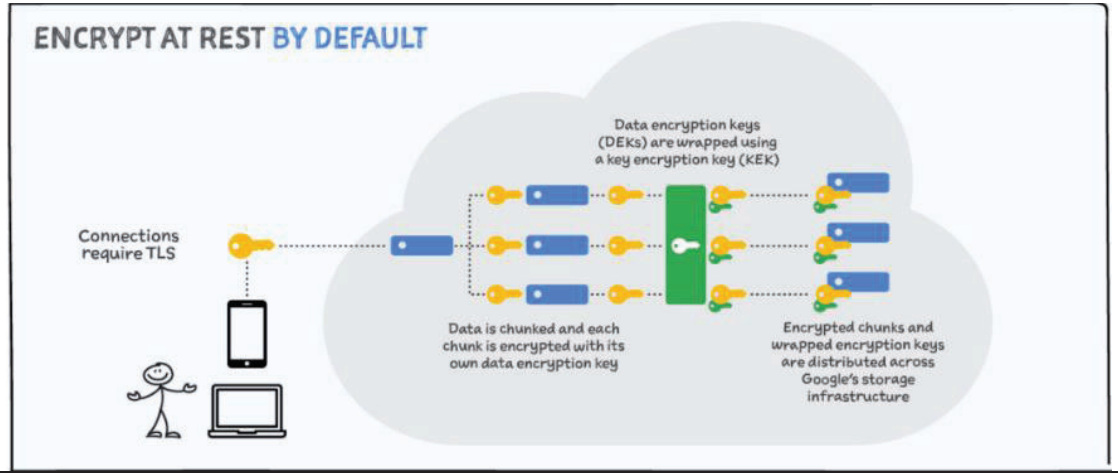
[51] SFI-GOOGLE_000005992, Google Cloud Tech, *How does encryption work at Google's data centers?*, YOUTUBE (Nov. 24, 2021), https://www.youtube.com/watch?v=82YD6esAK0o.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	 SFI-GOOGLE_000003146 at -149; *see also* SFI-GOOGLE_000005743 (Cloud Key Management System).
1[b][iv] reconstitute the dataset from at least a portion of the plurality of shares stored on the physical storage devices in response to a request from the client device for information in the dataset.	Google's "Encryption at Rest" comprises a secure storage system configured to reconstitute the dataset from at least a portion of the plurality of shares stored on the physical storage devices in response to a request from the client device for information in the dataset. Google has also explained the operation of this system as follows: > So first, how does [decryption and access of data] work in practice? So you can think about this as being three different actors here. There's a service that's using the data. There is a storage system that's storing the encrypted data. And there's a KMS that's storing . . . the key encryption keys. So what happens in practice is the service asks the storage system for some object. The storage system verifies that the service has the right to access that object, figures out all the chunks in which that data is stored, checks those ACLs. Then it pulls the data encryption keys that are sitting with those chunks of data, and passes those data encryption keys, encrypted, to the KMS. The KMS then verifies that the storage system--again, another ACL check--that it has the right to access those key encryption keys, decrypts those data encryption keys in memory, sends them back to the storage system. . . . Then from the storage system back to the service, the storage system

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	decrypts the data, and sends back the plaintext data to the service, in most cases. In some cases, the service decrypts it directly. SFI-GOOGLE_000003191 at 8:47-9:59, Google Cloud Tech, *Managing encryption of data in the cloud (Google Next '17)*, YOUTUBE (Mar. 10, 2017), https://www.youtube.com/watch?v=StJ1NOQjAjo&t=365s. As an example, after a Google application or service "makes a call to the storage system," the storage system "identifies the chunks in which that data is stored (the chunk IDs) and where they are stored," "pulls the wrapped DEK that is stored with [each] chunk," unwraps the DEK using the KEK, and Keystore "passes the unwrapped DEK back to the storage system, which decrypts the data chunk" and passes it to the requesting service or application. SFI-GOOGLE_000003146 at -152-153. Once all the chunks that compose a specific file or data structure are decrypted, "the data [is] available to the requesting application." SFI-GOOGLE_000003287 at -293; *see also* SFI-GOOGLE_000005743 (Cloud Key Management System).
Claim 2[pre] The secure storage network of claim 1.	Google's "Encryption at Rest" comprises the secure storage network of claim 1. *See* Claim 1, *supra*.
2[a] wherein the secure storage system is further configured to generate the plurality of shares by performing a cryptographic operation on the dataset.	Within Google's "Encryption at Rest," the secure storage system is further configured to generate the plurality of shares by performing a cryptographic operation on the dataset. For example, Google generates the plurality of shares by performing a cryptographic operation on the dataset received from the client device and distributing the dataset in the shares through its DEK/KEK system. For example, Google explains that "[e]ach chunk is encrypted at the storage level with an individual data encryption key (DEK)." SFI-GOOGLE_000003146 at -148; *see also id*. ("Google encrypts data before it is written to a database storage system or hardware disk. Encryption is inherent in all of our storage systems, rather than added afterward."). 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." *Id*. at -151; *see also* SFI-GOOGLE_000005743 (Cloud Key Management System). Below is an exemplary image from the Google Cloud webpage showing how data is "chunked" and "encrypted":

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	 SFI-GOOGLE_000003146 at -149.
Claim 4[pre] The secure storage network of claim 1,	Google's "Encryption at Rest" comprises the secure storage network of claim 1. *See* Claim 1, *supra*.
4[a] wherein the secure storage system is further configured to provide access to the reconstituted dataset.	Within Google's "Encryption at Rest," the secure storage system is further configured to provide access to the reconstituted dataset. Google has also explained the operation of this system as follows: > So first, how does [decryption and access of data] work in practice? So you can think about this as being three different actors here. There's a service that's using the data. There is a storage system that's storing the encrypted data. And there's a KMS that's storing . . . the key encryption keys. So what happens in practice is the service asks the

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	storage system for some object. The storage system verifies that the service has the right to access that object, figures out all the chunks in which that data is stored, checks those ACLs. Then it pulls the data encryption keys that are sitting with those chunks of data, and passes those data encryption keys, encrypted, to the KMS. The KMS then verifies that the storage system--again, another ACL check--that it has the right to access those key encryption keys, decrypts those data encryption keys in memory, sends them back to the storage system. . . . Then from the storage system back to the service, the storage system decrypts the data, and sends back the plaintext data to the service, in most cases. In some cases, the service decrypts it directly. SFI-GOOGLE_000003191 at 8:47-9:59; *see also* SFI-GOOGLE_000005743. As an example, after a Google application or service "makes a call to the storage system," the storage system "identifies the chunks in which that data is stored (the chunk IDs) and where they are stored," "pulls the wrapped DEK that is stored with [each] chunk," unwraps the DEK using the KEK, and Keystore "passes the unwrapped DEK back to the storage system, which decrypts the data chunk" and passes it to the requesting service or application. SFI-GOOGLE_000003146 at -152-53. Once all the shares that compose a specific file or data structure are decrypted, "the data [is] available to the requesting application." SFI-GOOGLE_000003287 at -293.
Claim 5[pre] The secure storage network of claim 1,	Google's "Encryption at Rest" comprises the secure storage network of claim 1. *See* Claim 1, *supra*.
5[a] wherein the secure storage system is further configured to establish a secure connection between the client device and the secure storage system.	Within Google's "Encryption at Rest," wherein the secure storage system is further configured to establish a secure connection between the client device and the secure storage system. For example, Google Cloud, prior to transmitting data between a client device and a storage destination, ensures the "authentication" of the data source, the "integrity" of the data upon arrival at its intended destination, and "encryption" of data while in transit to ensure its privacy. *See* SFI-GOOGLE_000005861, Google Cloud, *Encryption in Transit in Google Cloud* at -865 (2017), https://cloud.google.com/static/docs/security/encryption-in-transit/resources/encryption-in-transit-whitepaper.pdf. "[W]hen a user sends a request to a Google Cloud Service," Google authenticates the

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	connection using, *e.g.*, "HTTPS with a certificate from a web (public) certificate authority." *Id.* at -872-873. As another example, during data transfer, "communications are secured between the user and the Google front end using TLS, which is a cryptographic protocol."[52] Below is an exemplary image showing required TLS connections between a user and Google Cloud.[53] 
Claim 7[pre] The secure storage network of claim 1,	Google's "Encryption at Rest" comprises the secure storage network of claim 1. *See* claim 1, *supra*.

[52] SFI-GOOGLE_000005992.

[53] 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.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
7[a] wherein the secure storage system is configured to reconstitute the received dataset from fewer than all of the shares.	Within Google's "Encryption at Rest," the secure storage system is configured to reconstitute the received dataset from fewer than all of the shares. For example, each data share encrypted by Google Cloud "is distributed across [Google's] storage systems and is replicated in encrypted form for backup and disaster recovery." SFI-GOOGLE_000003146 at -149; *see also* SFI-GOOGLE_000005992. Google's encryption at rest is configured to reconstitute the dataset from fewer than all of the shares when it, for example, reconstitutes the data without using the backup copies of the shares of the same dataset.
Claim 8[pre] The secure storage network of claim 1,	Google's "Encryption at Rest" comprises the secure storage network of claim 1. *See* claim 1, *supra*.
8[a] wherein the secure storage system is configured to secure the dataset by encrypting the dataset using the at least one session key.	Within Google's "Encryption at Rest," the secure storage system is configured to secure the dataset by encrypting the dataset using the at least one session key. For example, Google Cloud uses symmetric encryption algorithms to secure the dataset, such as AES-GCM (256 bits) protocol for encryption at rest of data using DEKs and KEKs. *See, e.g.*, SFI-GOOGLE_000003146 at -156. 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." *Id*. at -151; *see also* SFI-GOOGLE_000005743. Below is an exemplary annotated image showing Google's securing of the dataset by encrypting the dataset using the session key, the DEK. *See* SFI-GOOGLE_000005816.

U.S. Patent No. 9,338,140	Google's "Encryption at Rest"[1]
	