IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

Security First Innovations, LLC, Plaintiff, v. Google LLC, Defendant.	Civil Action No. _____

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Security First Innovations, LLC ("SFI") files this complaint for patent infringement pursuant to 35 U.S.C. §§ 100 *et seq*. against Defendant Google LLC ("Google"), for infringement of U.S. Patent Nos. 10,452,854 ("the '854 Patent"), 11,068,609 ("the '609 Patent"), 11,178,116 ("the '116 Patent"), and 9,338,140 ("the '140 Patent") (collectively "the Asserted Patents") and alleges as follows:

NATURE OF THIS ACTION

1. This is an action for patent infringement arising under 28 U.S.C. § 1331 and the United States Patent Act, 35 U.S.C. § 100 *et seq*. SFI seeks damages and other appropriate relief for Defendant's widespread infringement of the Asserted Patents by Defendant's Google Cloud system.

IPR2025-01202
IBM v. Security First Innovations, LLC
IBM's Exhibit 1042
EX1042, Page 1

THE PARTIES

2. Plaintiff SFI is a limited liability company duly organized and existing under the laws of the Commonwealth of Virginia. SFI is located at 44095 Pipeline Plaza, Suite 140, Ashburn, Virginia 20147.

3. On information and belief, Defendant Google is a corporation duly organized and existing under the laws of the State of Delaware, having executive offices at 1600 Amphitheatre Parkway, Mountain View, California, 94043, and a regular and established place of business in the Eastern District of Virginia, including at 1900 Reston Metro Plaza, Reston, Virginia 20190.

FACTUAL BACKGROUND

A. Data Security & Encryption

4. The security of the important, valuable, private, or even simply personal, has been a primary concern for thousands of years. From treasure keeps securing gold, to bank vaults securing currency, to home intruder systems securing personal belongings, methods of security have evolved alongside what has needed to be secured.

5. Today, as more and more information is stored online through the use of computer technology, information is now atop the list of things which need securing. Generally known as "data security," the protection of information is of the utmost importance to those seeking to safeguard their important, valuable, private, and/or personal information.

6. Just as physical security has evolved, so too has data security. At a high level, data is generally either At-Rest or In-Transit. Each category comes with its own set of challenges relating to security, but in either category a popular way of securing digital data is called encryption. Encryption At-Rest refers to encrypting data that is stored on disk or other media,

such as, for example, data generally residing in computer storage. Encryption In-Transit refers to encrypting data that is in motion, generally being transferred between users or devices.

7. Encryption At-Rest, for example, is a critical component of outsourced computing systems (today generally referred to as cloud storage systems). Cloud storage is a method of computer data storage that generally allows for the outsourcing of data storage to a cloud storage provider. That data is ultimately accessed from that provider, being transferred through the Internet or private networks. Generally, the data is stored using physical servers that are operated by a third party, such as Google, for example. Employing Encryption At-Rest in server-based cloud storage systems comes with many challenges, including those related to latency, or limited bandwidth.

8. At a very high level, encryption works by transforming data from human-readable "plaintext" into "ciphertext" using a specific algorithm and "cryptographic key." The ciphertext is, in essence, illegible to anyone without the cryptographic key to transform the ciphertext back into plaintext. As explained by Google itself, "[a]t its most basic level, encryption is the process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it."[1]

9. Encryption serves several important functions. For example, encryption is not only used to protect data (because malevolent actors without the cryptographic key cannot access it); it can also be used to verify/authenticate the data (because if the key does not decrypt it, the data may have been altered).

[1] *What is encryption?* Google Cloud. https://cloud.google.com/learn/what-is-encryption (last visited Mar. 10, 2023)

10. There are many different methods of encrypting data, but the common thread is that in order to translate the encrypted data back into a usable format, a cryptographic key is required. With the right cryptographic key, anyone can access the data from the ciphertext.

11. As a result, "key management" is critical to the effectiveness of any cryptographic-based data security infrastructure. As explained by Google, "[e]ncryption is much less effective if the cryptographic keys that encrypt and decrypt the data are not secure. Malicious actors often concentrate their attacks on obtaining an organization's encryption keys. In addition to malicious actors, losing encryption keys (such as during a natural disaster that compromises servers) can lock organizations out of important data. This is why a secure key management system is often used by organizations to manage and secure their keys."[2]

12. Encryption alone is not always enough, particularly for sensitive data. Having complementary obfuscation techniques, along with encryption, is critical to providing an effective overall data security system.

13. The Asserted Patents describe and claim novel inventions that address, *inter alia*, data security and the challenges associated with securing data, including those specifically related to an innovative key management system. The Asserted Patents stem from the inventors' data security systems developed at Security First Corporation.

B. <u>Security First Corporation</u>

14. Security First Corporation ("SFC"), the original owner of the Asserted Patents, was established in 2002 to develop innovative data security systems.

15. From its inception, SFC focused on securing data, first focusing on biometric data, and then later realizing that the state of security in cloud computing, generally, was woefully

[2] *Id*.

inadequate. The Asserted Patents focus on solving those inadequacies by, among other things, unconventionally parsing and splitting the data into different portions before storage. Inventors named on the Asserted Patents were members of the original founding team behind SFC, and worked for years to develop a multi-layered data security system which refined and combined the concept of splitting data with the concept of data encryption. The inventions claimed by the Asserted Patents, as well as scores of other SFC patents, are a result of those efforts.

16. Over the years, SFC created an assortment of products offering data security solutions including, for example, the SPxSHARC, SPxGateway, and SPxClient. These products were a part of SFC's suite of end-to-end solutions for data security, protecting edge devices, point of sale, enterprise, cloud, networks, and more. SFC's technology has also been licensed and used by several companies to improve their data security including, for example, Unisys and IBM.

17. In 2022, SFI acquired the patents that originated at SFC, and today is their sole assignee. SFI was formed by the longtime former chairman of SFC.

C. <u>The Claimed Technology</u>

18. The inventions claimed in the Asserted Patents relate to a system for securing data from unauthorized access or use. *See e.g.*, '854 Patent at 1:25-26. More specifically, the inventions claimed in the Asserted Patents provide, among other things, solutions to common problems relating to prior art data security systems.

19. The Asserted Patents explain that "individuals and businesses conduct an ever-increasing amount of activities on and over computer systems." *See e.g.*, *id*. at 1:30-32. Because these systems "are often storing, archiving, and transmitting all types of sensitive information . . . an ever-increasing need exists for ensuring data stored and transmitted over these systems cannot be read or otherwise compromised." *See e.g.*, *id*. at 1:33-37.

20. As discussed above, encrypting data is a common method for providing enhanced security. There are many different ways of encrypting data—for example, the Asserted Patents explain that "[o]ne popular cryptography system is a public key system that uses two keys, a public key known to everyone and a private key known only to the individual or business owner thereof. Generally, the data encrypted with one key is decrypted with the other and neither key is recreatable from the other." *See e.g.*, *id*. at 1:54-59. As another example, biometrics may be included as part of the cryptographic system authentication process. *See e.g.*, *id*. at 2:14-25.

21. These prior art cryptographic systems have several flaws. For example, "typical public-key cryptographic systems are still highly reliant on the user for security." *See e.g.*, *id*. at 1:60-62. The Asserted Patents explain that "[u]nsophisticated users . . . generally store the private key on a hard drive accessible to others, . . . may choose poor names for files containing their private key, . . . [or] may save his or her private key on a computer system configured with an archiving or backup system, potentially resulting in copies of the private key traveling through multiple computer storage devices or other systems." *See e.g.*, *id*. at 1:64-2:8. Further, "many applications provide access to a user's private key through, at most, simple login and password access," which "provide little security." *See e.g.*, *id*. at 2:10-13; 1:43-45. Even biometric cryptographic systems suffer from a variety of drawbacks. "For example, the mobile user may lose or break the smartcard or portable computing device, thereby having his or her access to potentially important data entirely cut-off. Alternatively, a malicious person may steal the mobile user's smartcard or portable computing device and use it to effectively steal the mobile user's digital credentials. On the other hand, the portable-computing device may be connected to an open system, such as the Internet, and, like passwords, the file where the biometric is stored may be

susceptible to compromise through user inattentiveness to security or malicious intruders." *See e.g.*, *id*. at 2:27-38.

22. The Asserted Patents describe and claim solutions to these problems by, among other things, using a secure data parser to split the data into multiple portions (*e.g.*, generating a plurality of data chunks based on the data set), encrypting the parsed data (data chunks) using distinct encryption keys, encrypting the distinct encryption keys using an external key, and storing the encrypted, parsed data with data indicative of at least one of the distinct encryption keys on different storage devices. *See e.g. id*. at Abstract, Claim 1. These steps were unconventional and non-generic, particularly in the context of large scale, server-based data storage.

23. The idea of securing a data set using encryption *after* the data set has been split into multiple portions or chunks, as is described in the Asserted Patents, would have been regarded as wholly unconventional at the time of the inventions. This is in part because performing the encryption/decryption operations on the individual portions that were formed when the original data set was split requires substantial additional processing over what would have been needed to simply encrypt the original single data set.

24. For example, Sanjay Ghemawat *et al.*, *The Google File System* 19-22 (Oct. 20, 2003) (paper presented at the 19th ACM Symposium on Operating Sys. Principles), *available at* https://research.google/pubs/pub51/ (the "GFS Paper"), describes Google's early distributed file system which did not envision the use of encryption at all. The GFS Paper described this system as "widely deployed within Google as the storage platform for the generation and processing of data used by our service as well as research and development that require large data sets." *Id*. In fact, it took Google another decade before it would finally encrypt its data At-Rest. *See infra* at ¶¶ 35-37.

25. As another example, even in the context of securing data using encryption, prior to the Asserted Patents it was unconventional to store "data indicative of at least one of the distinct encryption keys" with the "plurality of data chunks." This would have been regarded as creating an insecurity by co-locating encrypted data with information which might facilitate decrypting such data. Despite that, however, some of the claimed inventions unconventionally store data indicative of at least one of the distinct encryption keys with the data chunks, which, among other advantages, provides certain unexpected benefits which enable the invention to be deployed effectively in a cloud environment. Plus, as another innovative example, and in order to further secure the data, certain of the claimed inventions innovatively perform a further encryption operation based on an external key from an external storage system.

26. As still another example, it would have also been unconventional to distribute the split data and the data indicative of the encryption keys across multiple different storage devices. This would have required developing an additional mechanism to locate the split data portions across the different storage devices, and then reassembling the data portions from the different storage devices (after decryption) in order to reconstitute the original data set. Certain claims of the Asserted Patents such as, for example, claim 1 of the '854 Patent, unconventionally require "storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different storage devices." *See e.g.*, '854 Patent at Claim 1.

27. In addition to providing solutions to the above-described problems, the claims of the Asserted Patents are directed to improving a basic function of a computer system—for example, the security of information on the computer system. For example, the claims of the '854 Patent require using an "external key from an external storage system" to perform a further

encryption operation to further secure previously split and encrypted data chunks.[3] This non-conventional step enables data indicative of the encryption keys to be securely stored with the data chunks since "the information may only be reassembled provided that all of the required shares and external encryption keys are present." '854 patent at 79:21-23. Storing data indicative of the encryption keys with the encrypted data improves efficiency of the decryption process since information needed to identify or locate the encryption keys is locally available with the data itself.

28. As a further example, the claims of at least the '854 Patent, '116 Patent, and the '609 Patent are further directed towards improvements in securing data in the specific context of cloud storage where many different sets of data are stored together. For example, through the disclosed and claimed proprietary key management system, certain claimed inventions allow for the secure sharing of data among different entities wherein only selected individuals are allowed to have access to the encrypted data as a whole. *See e.g.* '854 Patent at 64:42-65:9.[4] For example, the specification of the '854 Patent explains that the concept of an external key (*e.g.*, a "workgroup key") "allows for enhanced protection of information assets by encrypting key information stored within the shares. Once this operation is performed, even if all required shares and external keys are discovered, an attacker has no hope of recreating the information without access to the workgroup key." *Id*. at 79:66-80:4.

[3] Similarly, claim 1 of the '609 Patent requires a "first key" and a "second key"; claim 1 of the '116 Patent requires "obfuscating each of the plurality of different encryption keys"; and claim 1 of the '140 Patent requires "performing a securing operation on the dataset received from the client device."

[4] Google similarly explains that its Cloud Storage Encryption At-Rest system "[p]rovides an important privacy mechanism for our customers. When data is encrypted at rest, it limits the access that systems and engineers have to the data." *Default Encryption at Rest*, Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption (Sept. 2022).

29. The claims of at least the '140 Patent build on those core data securing innovations by claiming additional innovations directed to visually presenting a user's stored data in a virtual disk on a client device in the form of a directory that is mapped to the data shares stored across the different storage devices.

30. Accordingly, the claimed inventions of the Asserted Patents improve the functions of a computer system and improve upon conventional cryptographic methods for at least the reasons set forth above.

31. In addition, the claims of the Asserted Patents are necessarily rooted in computer technologies and provide technical and practical solutions to overcome problems associated with prior art cryptographic systems. The claimed systems and methods are rooted in computer technologies at least because, for example, they are directed to improving security of data storage in a computer system.

32. For at least the foregoing reasons, the elements of the claims of the Asserted Patents, individually or as part of an ordered combination, cover non-routine, unconventional, inventive features that provide specific technical and practical improvements to solve a particular problem in the field of information security.

D. <u>Google Cloud</u>

33. Google provides a suite of services generally referred to as Google Cloud. Google Cloud "consists of a set of physical assets, such as computers and hard disk drives, and virtual resources, such as virtual machines (VMs), that are contained in Google's data centers around the

globe."[5] An important part of the Google Cloud is Google Cloud Storage, which "is a service for storing your [data] in Google Cloud."[6]

34. On information and belief, Cloud Storage first launched in 2010.[7]

35. On information and belief, at its inception, Google did not encrypt the data stored on Google Cloud. On information and belief, this decision not to encrypt the data was made because, for example, "encrypting information while it is stored would prevent Google from showing the right online advertisements to users."[8]

36. On information and belief, Google's lack of encryption combined with allegations of Google's involvement in the National Security Agency's PRISM program (which, on information and belief, was related to Google's lack of encryption) led to reduced public trust in Google Cloud Storage.[9]

---

[5] *Google Cloud Overview*, https://cloud.google.com/docs/overview (last visited Mar. 10, 2023)

[6] *What Is Cloud Storage?*, Google Cloud, https://cloud.google.com/storage/docs/introduction (last visited Mar. 10, 2023)

[7] Reto Meier, *An Annotated History of Google's Cloud Platform*, Medium (Feb. 10, 2017), https://medium.com/@retomeier/an-annotated-history-of-googles-cloud-platform-90b90f948920; Sean Lynch, *Announcing Google App Engine for Business*, Google Code: The Official Google Code Blog (May 19, 2010), http://googlecode.blogspot.com/2010/05/announcing-google-app-engine-for.html.

[8] Amir Efrati, *Why Google Doesn't Encrypt User Data While Stored*, Wall St. J. (July 31, 2013), https://www.wsj.com/articles/BL-DGB-28206.

[9] *See* Barton Gellman and Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html; Farhad Manjoo, *Et Tu, Silicon Valley?*, Slate (June 7, 2013, 4:28 PM) https://slate.com/technology/2013/06/prism-apple-google-microsoft-how-the-nsa-s-surveillance-program-could-ruin-silicon-valley.html; *see also* Declan McCullagh, *Google Tests Encryption to Protect Users' Drive Files Against Government Demands*, CNET (July 17, 2013, 10:47 AM) https://www.cnet.com/tech/tech-industry/google-tests-encryption-to-protect-users-drive-files-

37. On information and belief, realizing the importance of encrypting data stored on Google Cloud, Google added server-side encryption to Google Cloud Storage in August of 2013.[10]

38. More recently, Google Cloud implements encryption technology in a manner which infringes the Asserted Patents. Google explains that it "encrypts all customer content stored at rest, without any action from you, using one or more encryption mechanisms."[11]

39. At a high level, Google's Encryption At-Rest implements the following steps: Data is broken into chunks for storage; each chunk is encrypted at the storage level with an individual data encryption key (DEK); and each chunk is distributed across Google's storage systems.[12] Google provides the following exemplary diagrams depicting these steps:

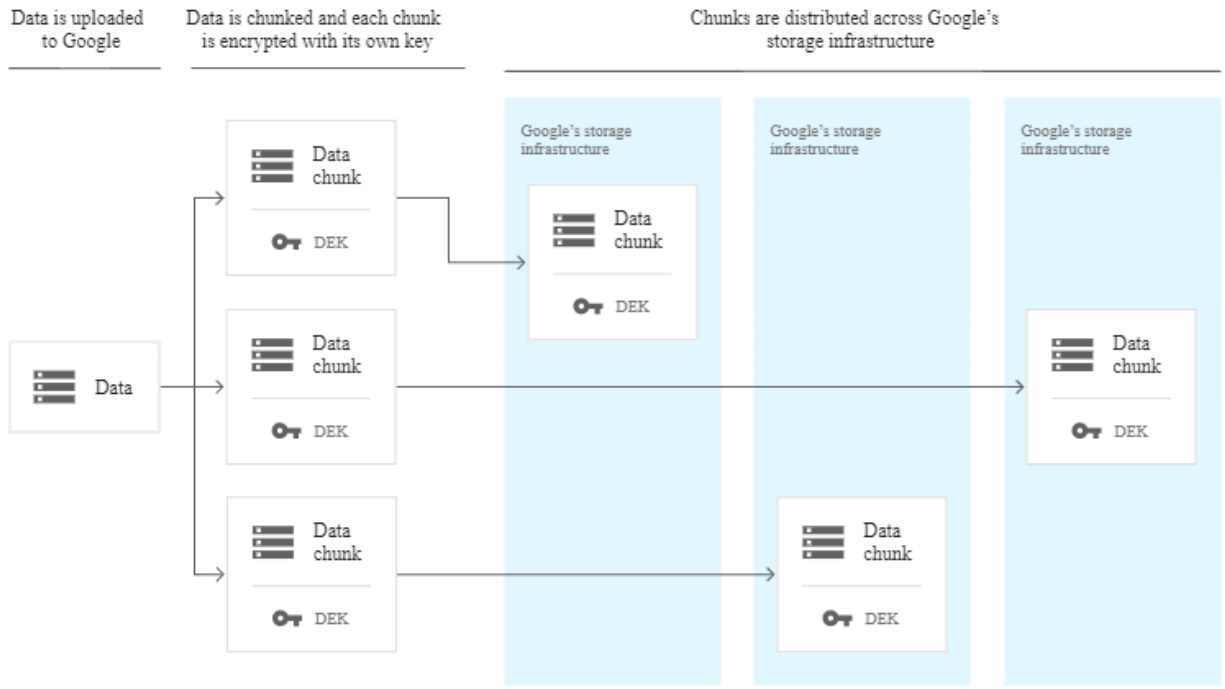
---

against-government-demands/ (explaining that encryption can protect data against unauthorized access, including from PRISM).

[10] Harrison Weber, *A Brief History of Encryption at Google*, VentureBeat (Apr. 21, 2014), https://venturebeat.com/dev/a-brief-history-of-encryption-at-google/.

[11] *Default Encryption at Rest*, Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption (Sept. 2022).

[12] *Id*.



40. Following some of the reasoning of SFC several years earlier, 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."[13]

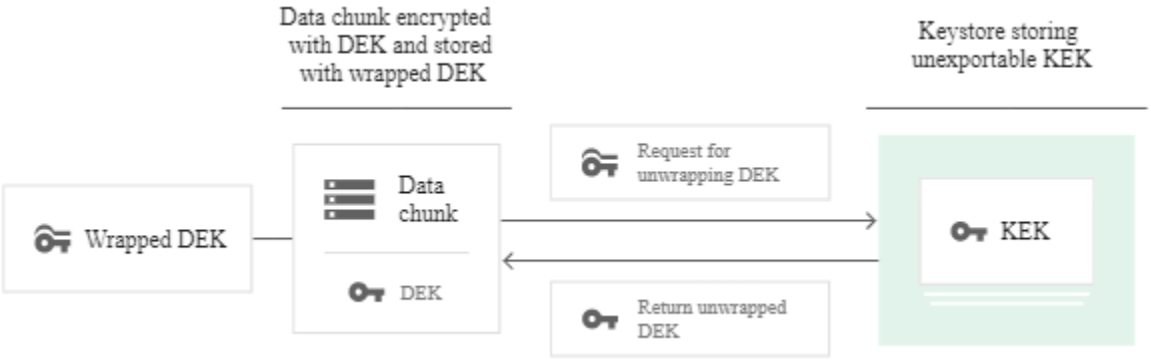
41. The DEK is then further encrypted with a key encryption key (KEK) that is stored centrally in a repository built specifically for storing keys, which Google refers to as "Keystore." Following the logic explained in the Asserted Patents, Google states that "[h]aving a smaller number of KEKs than DEKs and using a central Keystore makes storing and encrypting data at our scale manageable, and lets us track and control data access from a central point."[14]

42. The process of decrypting a data chunk therefore requires retrieving the encrypted DEK, sending that to Keystore, unencrypting the DEK and sending it back to the storage device,

[13] *Id.*

[14] *Id.*

then using that unencrypted DEK to unencrypt the data chunk. Google provides the following diagram depicting these steps:



43. The chain of encryption does not end there, as the KEK itself is sent to and received by a Root Keystore where it is encrypted for further security:

> Keystore is protected by a root key called the *keystore master key*, which wraps all of the KEKs in Keystore. This keystore master key is AES-256 and is itself stored in another key management service, called Root Keystore. (In the past, the keystore master key was AES-128, and some of these keys remain active for decrypting data.) Root Keystore stores a much smaller number of keys—approximately a dozen per region. For additional security, Root Keystore isn't run on general production machines, but instead is run only on dedicated machines in each Google data center.[15]

44. As explained below, Google Cloud Storage infringes the Asserted Patents.

JURISDICTION AND VENUE

45. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, Title 35 United States Code, including 35 U.S.C. § 1 *et seq*. This complaint includes claims for patent infringement arising under the patent laws of the United States, including 35 U.S.C. § 271 *et seq*.

46. This Court has personal jurisdiction over Google because Google makes, uses, offers for sale, and/or provides products and services in the Eastern District of Virginia, has

[15] *Id*.

committed and continues to commit acts of infringement in the Eastern District of Virginia, owns land in the Eastern District of Virginia, has conducted and continues to conduct business in the Eastern District of Virginia, including by maintaining a physical presence and regular place of business in Reston, Virginia, and/or has engaged in continuous and systematic activities in the Eastern District of Virginia. On information and belief, Google derives substantial revenue from the acts of infringement in the Eastern District of Virginia and derives substantial revenue from interstate and international commerce associated with the infringing products.

47. Venue is proper in this judicial District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 35 U.S.C. § 1400(b) at least because Google has committed and continues to commit acts of infringement within this District giving rise to this action and has a regular and established place of business in this judicial district, including an office space located at 1900 Reston Metro Plaza, Reston, VA 20190. Furthermore, Google has provided and continues to provide infringing products and/or services to residents, businesses, and government agencies located in this District.

48. As discussed above, the relevant technology in this case includes the encryption technology system implemented by Google Cloud Storage, specifically as implemented on servers in Google data centers located in this District. Due in part to Virginia's uniquely significant role in the infringing systems, the Eastern District of Virginia has a strong interest in this case.

49. Google touts that "Virginia is home to the largest concentration of data centers in the world," a "community" that "Google is proud to be part of."[16] The Northern Virginia Technology Council's most recent report on the economic impact of data centers in Virginia

[16] *Data Center Alley*, Google Data Ctrs., https://www.google.com/about/datacenters/locations/loudoun-county/#:~:text=Data%20center%20alley,be%20part%20of%20this%20community (last visited Mar. 10, 2023).

concluded that in 2021, data centers drove "62 percent" "of all the new investment" in Virginia, supported over 45,000 jobs, and drove $15.3 billion in economic output.[17]

50. Because, as Google recognizes, the Eastern District of Virginia is extremely important to the technology at issue, Google maintains a significant presence in the District. As discussed in more detail below, Google has, among other things, employed hundreds of Virginians at its office in Reston, invested over $1 billion into data center development in the District, and partnered with and acquired companies headquartered in the District that help it develop and sell cloud storage products and services that infringe the Asserted Patents.

51. Google has maintained its Reston, Virginia office since 2005.[18] In 2019, Google announced its new office space at 1900 Reston Metro Plaza, Reston, VA 20190.[19] At that time, Google reported that it had "close to 200 employees" in Reston "working on major projects across engineering, sales and more."[20] In 2021, Google leased another floor at 1900 Reston Metro Plaza,

---

[17] *The Impact of Data Centers on the State and Local Economies of Virginia*, N. Va. Tech. Council 4-5 (2022) [accessible at https://www.nvtc.org/NVTC/Workforce/Resource_Library_Docs/2022_NVTC_Data_Center_Report_Download.aspx].

[18] Gregg MacDonald, *Google Takes Top Two Floors of Reston Station Building*, Fairfax Cnty. Times (Apr. 12, 2019), https://www.fairfaxtimes.com/articles/google-takes-top-two-floors-of-reston-station-building/article_199ca682-5d5b-11e9-ab80-5b7a2a6ce62f.html.

[19] Catherine Douglas Moran, *Here's a Look Around Google's New Reston Station Office Space*, Reston Now (Mar 22, 2019, 9:45 AM), https://www.fairfaxtimes.com/articles/google-takes-top-two-floors-of-reston-station-building/article_199ca682-5d5b-11e9-ab80-5b7a2a6ce62f.html.

[20] Catherine Couglas Moran, *Google Moving to New Reston Station Office Space This Summer*, Reston Now (Apr. 8, 2019, 1:15 PM), https://www.fairfaxtimes.com/articles/google-takes-top-two-floors-of-reston-station-building/article_199ca682-5d5b-11e9-ab80-5b7a2a6ce62f.html.

"bringing the total footprint in the building to approximately 115,000 square feet."[21] As of the date of this complaint, Google is seeking to add 67 "Engineering & Technology" jobs to its Reston workforce, including a "Security Architect, Google Cloud," a "Security Platform Engineer, Google Cloud," a "Senior Security Consultant, Google Cloud," a "Cloud Infrastructure Engineer, Global Public Sector, Google Cloud," and a "Cloud Data Engineer, Global Public Sector, Professional Services," among dozens of others.[22]

52. In total, Google has "more than 480 employees in Virginia, overseeing critical functions like Google Cloud,"[23] including senior directors of engineering, senior software engineers and data center technicians located in the Eastern District of Virginia. In 2021 alone, these employees helped Google provide "[m]ore than 475,000 Virginia businesses" with "direct connections to their customers."[24]

53. Beyond its significant employee presence, Google maintains at least two data centers in this District located in Loudoun County. Google purchased 148 acres of land in Loudoun County for approximately $70 million in 2017 to house these data centers,[25] and has

---

[21] Fatimah Waseem, *Just In: Google to Lease More Space at Reston Station*, Reston Now (Mar. 18, 2021, 10:50 AM), https://www.restonnow.com/2021/03/18/just-in-google-to-lease-more-space-at-reston-station/.

[22] *Reston*, Google Careers, https://careers.google.com/locations/reston/ (last visited Mar. 10, 2023).

[23] Michael O'Connell, *Google to Invest Over $300M in VA to Improve Education, Job Training*, Patch: Reston VA (Apr. 19, 2022, 2:28 PM), https://patch.com/virginia/reston/video-youngkin-shoots-hoops-gw-basketball-alum-google-event.

[24] *Virginia*, Google Econ. Impact, https://economicimpact.google.com/state/va/ (last visited Mar. 10, 2023).

[25] Sydney Kashiwagi, *Google Purchases 148 Acres in Loudoun County for Two New Data Centers*, Loudoun Times-Mirror (Nov. 29, 2017), https://www.loudountimes.com/news/google-purchases-148-acres-in-loudoun-county-for-two-new-data-centers/article_9ea96f08-75b1-5779-9fcf-

since invested approximately $1.8 billion into constructing and maintaining them, including a $600 million investment in 2021.[26]

54. These data centers play a critical, uniquely relevant role to the infringing systems and products Google offers its customers, including those customers located in this District. Google lists, by region, the specific products and services offered by its data centers. The data center region located in the Eastern District of Virginia is referred to as "us-east4," which is located in Ashburn, Virginia (in Loudoun County).[27] No Google data center in the Americas offers more combined "Storage & Databases" and "Identity & Security" services than Google's $1.8 billion data centers in Loudoun County.[28] Through these data centers, Google offers "Cloud Key Management," "Key Access Justifications," "Cloud Storage," and "Storage Transfer Service" products and services, among many others.[29]

---

e2b1dec8429e.html#:~:text=Tech%20giant%20Google%20has%20purchased,has%20spent%20%2439%20million%20on.

[26] Amber Styles, *Google Announces $600M Data Center Expansion in Loudoun County*, Loudoun Cnty. Dep't Econ. Dev. (Mar. 18, 2021), https://biz.loudoun.gov/2021/03/18/google-600-million-data-center-expansion-loudoun/.

[27] *Regions and Zones*, Google Cloud, https://cloud.google.com/compute/docs/regions-zones (last visited Mar. 10, 2023).

[28] *Products Available by Location*, Google Cloud, https://cloud.google.com/about/locations#americas (last visited Mar. 10, 2023).

[29] *Id*. These services are directly relevant to the infringing products and systems. "Cloud Key Management Service allows [Google's customers] to create, import, and manage cryptographic keys and perform cryptographic operations in a single centralized cloud service." *Cloud Key Management Service Documentation*, Google Cloud, https://cloud.google.com/kms/docs#:~:text=Cloud%20Key%20Management%20Service%20allows,a%20single%20centralized%20cloud%20service (last visited Mar. 10, 2023). "Key Access Justifications" "works together with [Google's] Cloud External Key Manage to . . . give[] customers a justification every time their externally hosted keys are used to decrypt data." Joseph Valente, *Key Access Justifications: A New Level of Control and Visibility*, Google Cloud (Nov. 20, 2019), https://cloud.google.com/blog/products/identity-security/control-access-to-gcp-data-with-key-access-justifications. "Cloud Storage always encrypts [Google's customers'] data on the server side," which "occurs after Cloud Storage receives [a customer's] data, but before the data is written a disk and stored." *Data Encryption Options*, Google Cloud,

55. Virginia also plays a critical role in the Google Cloud infrastructure due to its geographical positioning. To move data to and from its various data centers, Google has chosen "to build the world's fastest undersea data connection" through Northern Virginia.[30] Google announced the "Dunant cable" in 2018, and reporters noted that it would "[b]oost [i]ts [c]loud" and "provide a high-bandwidth path for Internet traffic from the west coast of France across the Atlantic, landing in [this District in] Virginia Beach," and that "[o]nce that traffic arrives in Virginia Beach, much of it will be forwarded to Loudoun County in Northern Virginia."[31]

56. Google's data security and storage presence in the Eastern District of Virginia is not just well established; it is growing. Google has been expanding its presence in the District through acquisitions of and partnerships with local companies working in this space. Last September, Google spent $5.4 billion to acquire Mandiant, Inc., headquartered in Alexandria, Virginia. Mandiant, "now part of Google Cloud," provides "Cloud Security," "Cyber Security Transformation," and "Cyber Risk Management" services.[32] Mandiant's CEO marked the acquisition as "a great moment for our team and for the security community we serve" and further noted that "[a]s part of Google Cloud, Mandiant now has a far greater capability to close the

---

https://cloud.google.com/storage/docs/encryption (last visited Mar. 10, 2023). "Storage Transfer Service" allows clients to "[m]ove or backup data to a Cloud Storage bucket either from other cloud storage providers or from a local or cloud POSIX file system" and "[u]ses TLS encryption" when transferring data. *What Is Storage Transfer Service?*, Google Cloud https://cloud.google.com/storage-transfer/docs/overview (last visited Mar. 10, 2023).

[30] Klint Finley, *How Google Is Cramming More Data into Its New Atlantic Cable*, Wired (Apr. 5, 2019, 9:00 AM), https://www.wired.com/story/google-cramming-more-data-new-atlantic-cable/.

[31] Rich Miller, *Google Building Trans-Atlantic Cable to Boost Its Cloud in Northern Virginia*, Data Ctr. Frontier (July 17, 2018), https://www.datacenterfrontier.com/cloud/article/11430110/google-building-trans-atlantic-cable-to-boost-its-cloud-in-northern-virginia.

[32] *Cyber Security Consulting Services*, Mandiant, https://www.mandiant.com/services/consulting (last visited Mar. 10, 2023).

security gap created by a growing number of adversaries. . . . By combining our expertise and intelligence with the scale and resources of Google Cloud, we can make a far greater difference in preventing and countering cyber attacks, while pinpointing new ways to hold adversaries accountable."[33]

57. Google's partnerships with dozens of local companies have further cemented its secure cloud technology presence in the Eastern District of Virginia. For example, DivvyCloud by Rapid 7 is an Arlington-based Google Cloud "Technology Partner" and independent software vendor that "protects . . . cloud and container environments from misconfigurations, policy violations, threats, and IAM challenges" while helping "customers achieve continuous security and compliance, and . . . fully realize the benefits of cloud and container technology."[34] Dinoct Inc. is another "Technology Partner" and independent software vendor headquartered in this District advertising "cloud security" services "with the core principle of build-once, deploy-often, and Infrastructure as Code method to build [a customer's] cloud platform on Google Cloud."[35] Similarly, Peer Software, Inc. (another independent software vendor and Google Technology Partner) is also located in this District and offers services to navigate the "increasingly complex array of storage infrastructure choices" and assists "IT administrators" in managing "the

---

[33] Kevin Mandia, *Moving the Mission Forward: Mandiant Joins Google Cloud*, Mandiant, https://www.mandiant.com/resources/blog/mandiant-joins-google-cloud (Jan. 4, 2023).

[34] *DivvyCloud by Rapid7*, Google Cloud, https://cloud.google.com/find-a-partner/partner/botfactory-from-divvycloud (last visited Mar. 10, 2023).

[35] *Dinoct Inc*, Google Cloud, https://cloud.google.com/find-a-partner/partner/dinoct-inc (last visited Mar. 10, 2023).

unenviable task of trying to architect, build and operate resilient, highly available 24/7 global operations."[36]

58. Google's relationship with relevant companies in this District is not limited to software development and service partners; Google Cloud also works with many "Reseller Partner[s]" in the Eastern District of Virginia to implement its secure cloud technology. Four Points Technology is one such "[r]eseller" headquartered in Fairfax County offering "Google Cloud Platform" and "Google Cloud" products "to help [its] Federal Government customers" with, among other things, "Data Center Consolidation," "Cloud Computing," and "Security" solutions.[37] AIS Network is a similar "[r]eseller" based in this District offering "cloud enablement, information security, [and] risk management" products while "serv[ing] more than 60,000 end users in the Commonwealth of Virginia."[38] Likewise, CVP offers "[c]ybersecurity" services and "[c]ompetencies [that] include security operations, cyber defense, cloud security, security automation and risk management,"[39] and ThunderCat Technology "provid[es] strategies for Infrastructure, Cyber Security, and Cloud Transformation,"[40] both located in this District.

59. In addition to its local "[r]eseller" partners, Google recently created a new subsidiary, "Google Public Sector," to offer "Google Cloud for the Federal Government" directly.

---

[36] *Peer Software, Inc.*, Google Cloud, https://cloud.google.com/find-a-partner/partner/peer-software-inc (last visited Mar. 10, 2023).

[37] *Four Points Technology*, Google Cloud, https://cloud.google.com/find-a-partner/partner/four-points-technology (last visited Mar. 10, 2023).

[38] *AIS Network*, Google Cloud, https://cloud.google.com/find-a-partner/partner/ais-network (last visited Mar. 10, 2023).

[39] *CVP*, Google Cloud, https://cloud.google.com/find-a-partner/partner/ais-network (last visited Mar. 10, 2023).

[40] *ThunderCat Technology*, Google Cloud, https://cloud.google.com/find-a-partner/partner/thundercat-technology (last visited Mar. 10, 2023).

Introduced in June of 2022, Google Public Sector already works with the Arlington-based Department of Defense, and Google advertises that its "defense-in-depth security protects the federal government's data at scale."[41] Google Public Sector's CEO is based in Fairfax County and works from Google's Reston office.[42]

60. In addition to the Eastern District of Virginia being a proper venue at the heart of this controversy, SFI is also at home in the District. SFI is a Virginia Domestic Limited-Liability Company headquartered at 44095 Pipeline Plaza, Suite 140, Ashburn, VA 20147.

FIRST CLAIM FOR RELIEF

(Infringement of U.S. Patent No. 10,452,854)

61. SFI repeats, re-alleges, and incorporates herein by reference the allegations of Paragraphs 1-60 of its Complaint.

62. On October 22, 2019, United States Patent No. 10,452,854 entitled "Secure Data Parser Method And System" duly and legally issued to inventors Mark S. O'Hare, Rick L. Orsini, Roger S. Davenport, and Steven Winick. A true and correct copy of the '854 Patent is attached to this Complaint as Exhibit A.

63. SFI is the owner by assignment of the entire right, title, and interest in and to the '854 Patent, including the right to seek damages and any remedies for past, current, and future infringement thereof.

---

[41] *Google for Government Solutions*, Google Cloud, https://cloud.google.com/solutions/federal-government (last visited Mar. 10, 2023).

[42] Robyn Sidersky, *Google Public Sector Taps Booz Allen Exec as CEO*, Va. Bus. (Sept. 22, 2022), https://www.virginiabusiness.com/article/booze-allen-exec-named-google-public-sector-ceo/ (last visited Mar. 10, 2023); Karen Dahut, LinkedIn, https://www.linkedin.com/in/karen-dahut-24135811 (last visited Mar. 10, 2023).

64. The '854 Patent claims priority to United States Provisional Application No. 60/738,231 filed on November 18, 2005.

65. The '854 Patent is valid and enforceable.

66. SFI is informed and believes, and on that basis alleges, that Google has infringed and is currently infringing one or more claims of the '854 Patent, in violation of 35 U.S.C. § 271 *et seq*.

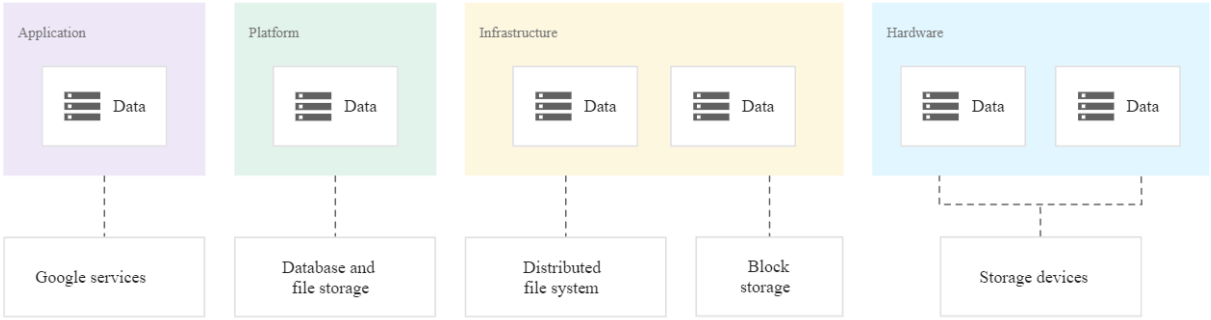
67. Google infringes literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) by, among other things, making, using, offering to sell, and/or selling within this District and elsewhere in the United States, without authority or license, Google products and services falling within the scope of one or more claims of the '854 Patent.

68. For example, as discussed below, the methods and products with which Google performs its encryption technology infringes at least Claim 1 of the '854 Patent.

Claim 1[pre]: A method for securely storing a data set, the method comprising:

69. Google meets the preamble (even if the preamble is not limiting). Google securely stores a data set by, for example, securely storing user data in Google Cloud.

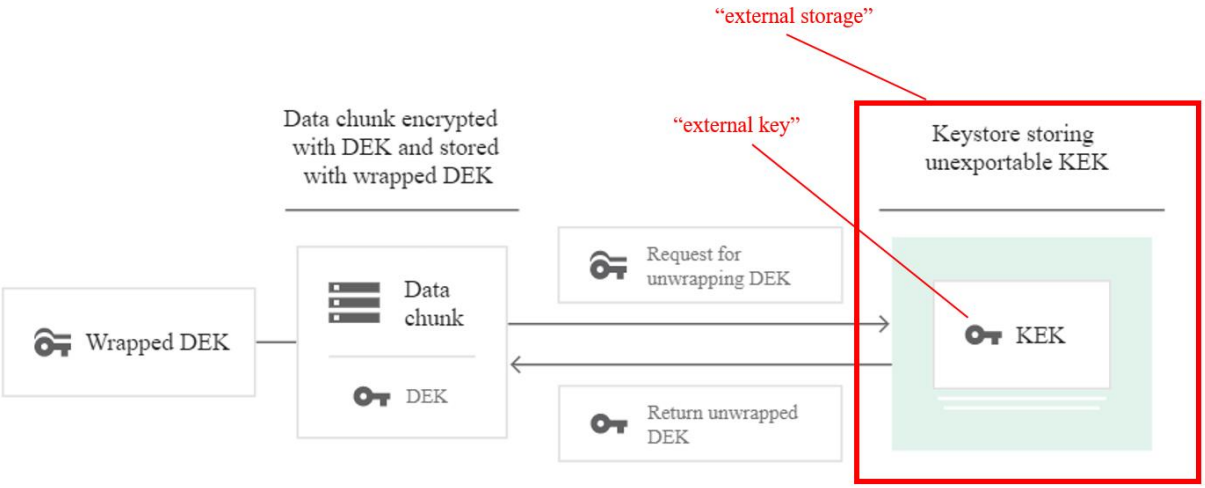
70. For example, Google states its "comprehensive security strategy includes encryption at rest" and it "encrypt[s] all Google customer content at rest, without any action required by [the customer], using one or more encryption mechanisms." Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption. Below is an exemplary image from the Google Cloud webpage showing "the several layers of encryption that are generally used to protect user data in Google production data centers."



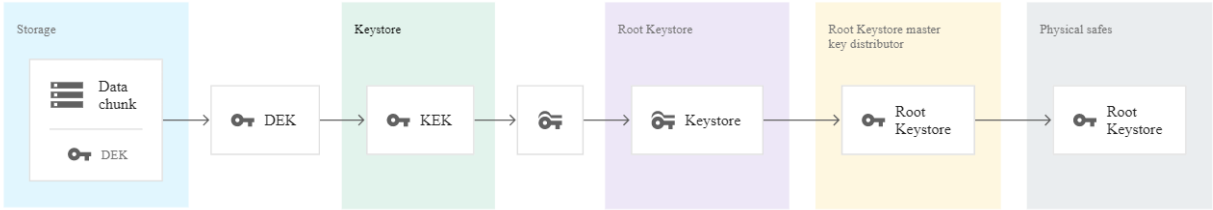
Claim 1[a]: receiving an external key from an external storage system,

71. Google meets this limitation. The Google products and method include receiving an external key from an external storage system. For example, Google's encryption technology uses an external key from an external storage system in the form of a Key Encryption Key ("KEK") which is stored in an external storage system Google refers to as "Keystore". *See id*. ("These KEKs are stored centrally in Keystore, a repository built specifically for storing keys."); *id*. ("When a storage system needs to retrieve encrypted data, it retrieves the wrapped DEK and passes it to Keystore. Keystore then verifies that this service is authorized to use the KEK and, if so, unwraps and returns the plaintext DEK to the service."). Below is an exemplary annotated image[43] from the Google Cloud webpage showing an example of an external key stored in external storage:

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



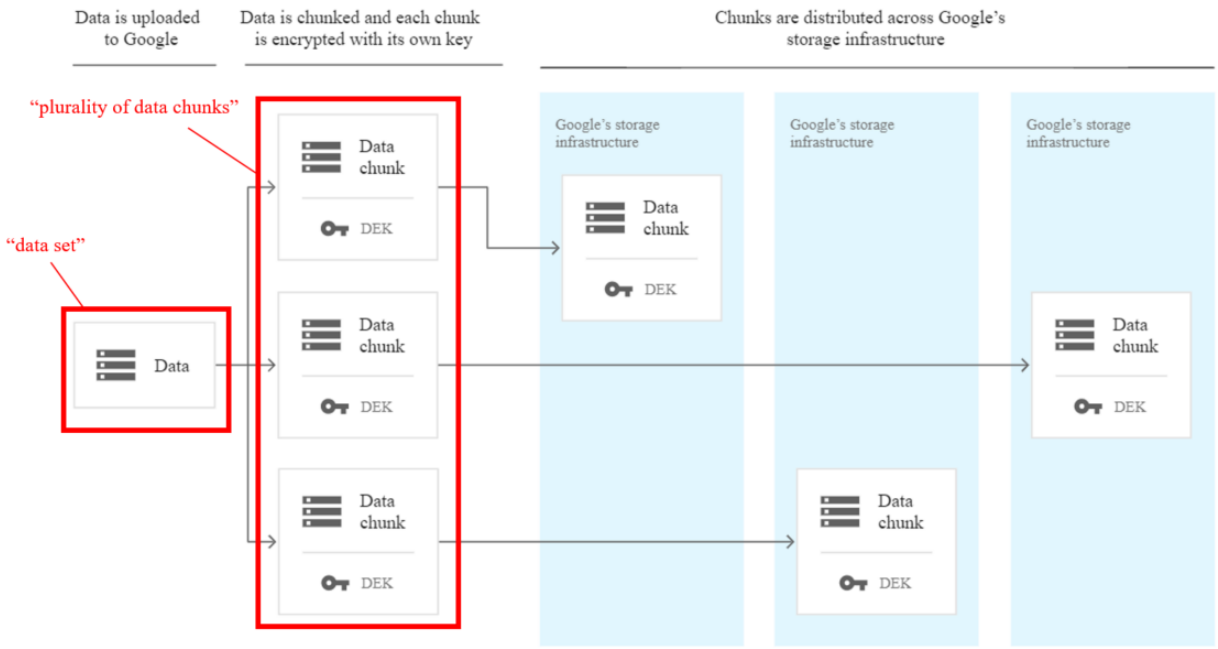
72. This external key is received by, for example, the Root Keystore. Google states that "Keystore is protected by a root key called the *keystore master key*, which wraps all of the KEKs in Keystore. This keystore master key is AES-256 and is itself stored in another key management service, called Root Keystore." *Id*. *See also id*. ("Keystore keys are wrapped with the Keystore master key, which is stored in Root Keystore."). The Root Keystore therefore receives the KEK in order to wrap and return it to Keystore. *See id*:



<u>Claim 1[b]: generating a plurality of data chunks based on the data set, such that the data set can be reconstructed using at least a minimum number of the plurality of data chunks, wherein generating the data chunks comprises:</u>

73. Google meets this limitation. The Google products and method include generating a plurality of data chunks based on the data set, such that the data set can be reconstructed using at least a minimum number of the plurality of data chunks. For example, Google generates a plurality of data chunks based on the data set by splitting user data set into data chunks. As a

further example, the data set can be reconstructed from the data chunks. *See id*. ("Data is broken into subfile chunks for storage"). Below is an exemplary annotated image from the Google Cloud webpage showing an example of a data set and plurality of data chunks:



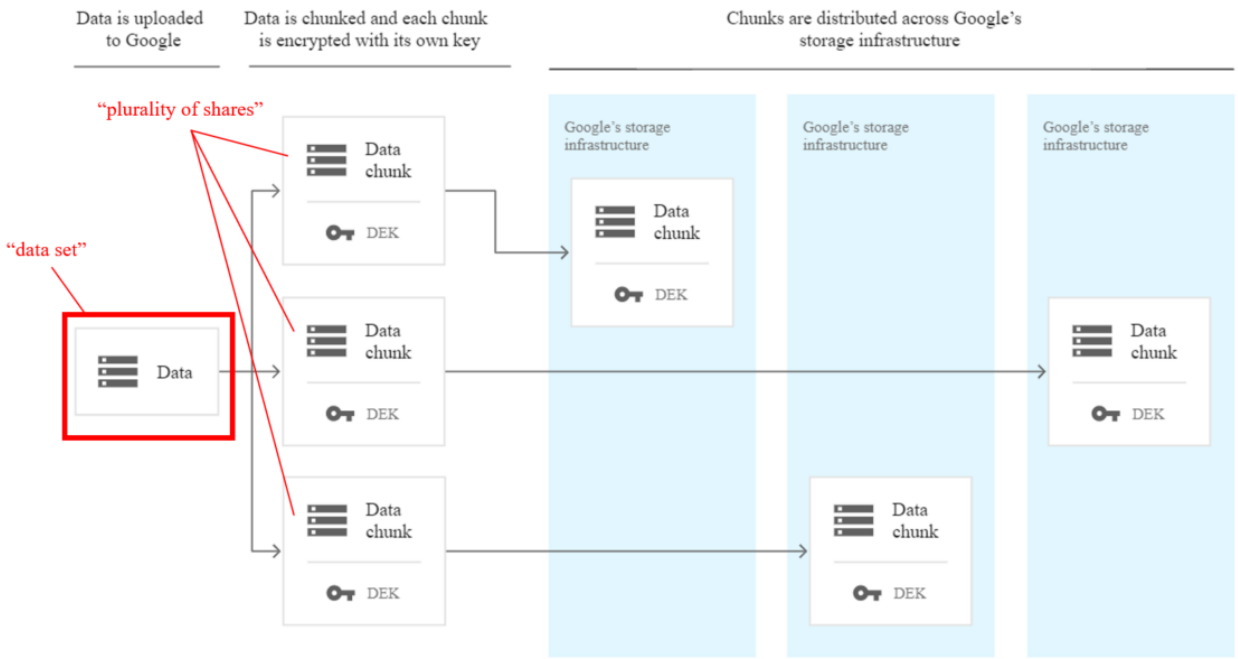
74. Google has explained the operation of this system as follows:

> So first, how does that 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 encryption keys--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 decrypts the data, and sends back the plaintext data to the service, in most cases. In some cases, the service decrypts it directly.

See Maya Kaczorowski, *Managing Encryption of Data in the Cloud*, YouTube (Mar. 10, 2017), https://www.youtube.com/watch?v=StJ1NOQjAjo at 8:47-9:59.

Claim 1[c]: distributing the data set into a plurality of shares, wherein each of the shares comprises less than all of the data set,

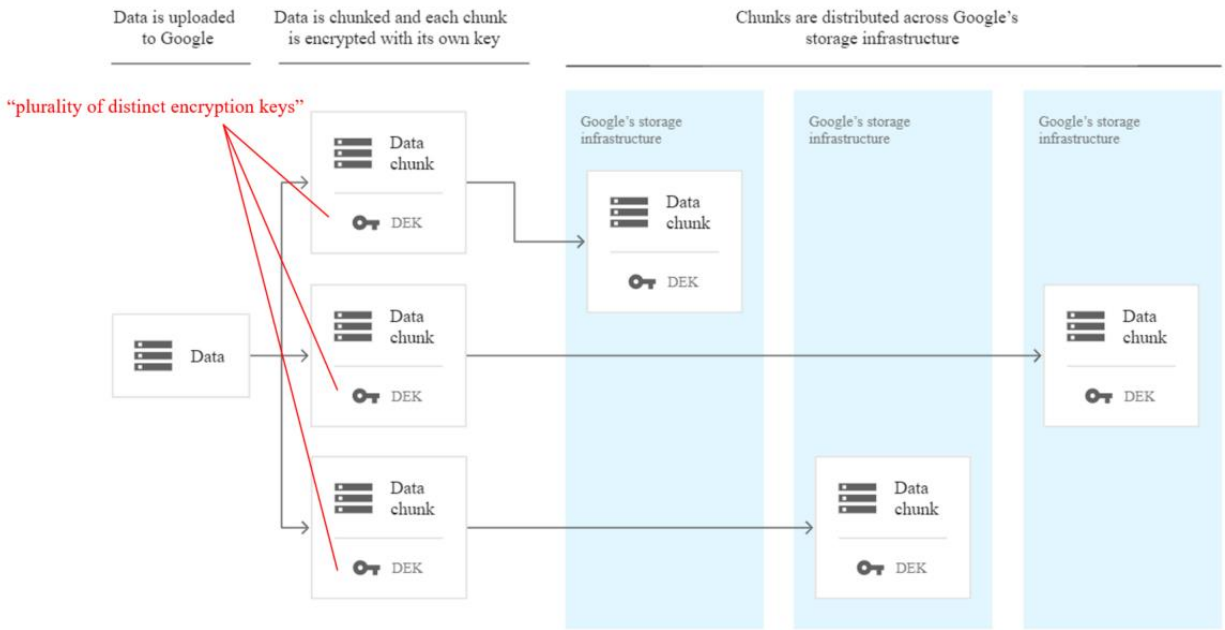
75. Google meets this limitation. The Google products and method include distributing the data set into a plurality of shares, wherein each of the shares comprises less than all of the data set. For example, Google distributes the data set into a plurality of shares as "[d]ata is broken into subfile chunks for storage." Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption. Each of the shares comprises less than all of the data set. *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing an example of a data set and plurality of shares:



Claim 1[d]: accessing a plurality of distinct encryption keys,

76. Google meets this limitation. The Google products and method include accessing a plurality of distinct 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." *Id*. 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." *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing an example of a plurality of distinct encryption keys:

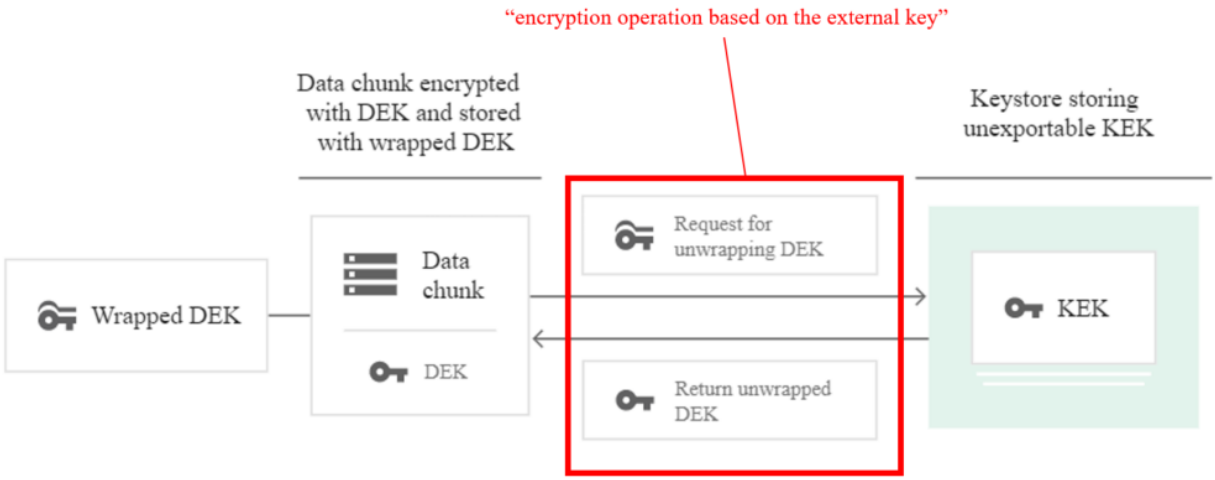


<u>Claim 1[e]: encrypting each of the shares with a respective one of the plurality of distinct encryption keys,</u>

77. Google meets this limitation. The Google products and method include encrypting each of the shares with a respective one of the plurality of distinct encryption keys. For example, Google's encryption technology encrypts each of the above-described shares with a distinct encryption key. *See supra* Claim 1[d]. Google explains that "[d]ata is chunked and each chunk is encrypted with its own key." *Default Encryption at Rest: Generating DEKs*, Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption#generating_deks (last visited Mar. 10, 2023).

Claim 1[f]: performing an encryption operation based on the external key to further secure the plurality of data chunks; and

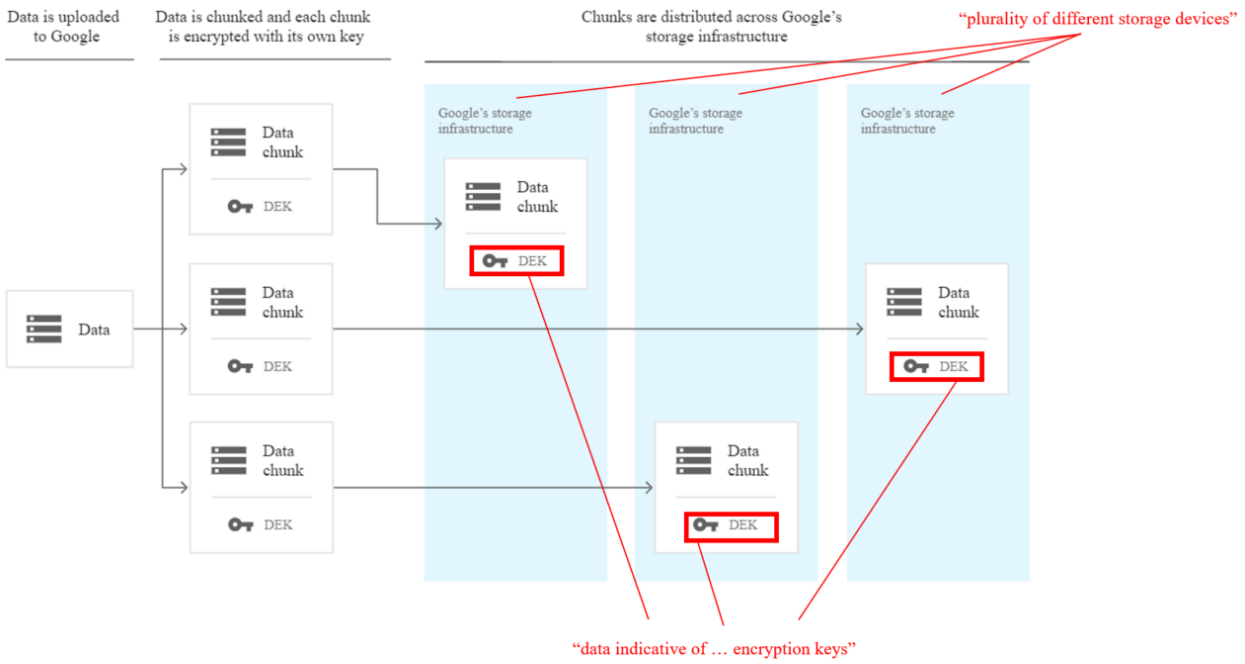
78. Google meets this limitation. The Google products and method include performing an encryption operation based on the external key to further secure the plurality of data chunks. For example, Google performs an encryption operation based on the external key to further secure the plurality of data chunks by encrypting each of the DEKs with a KEK. Google explains that "DEKs are encrypted with (wrapped by) a key encryption key (KEK)." *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing an example of an encryption operation based on the external key:



Claim 1[g]: storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different storage devices.

79. Google meets this limitation. The Google products and method include storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different storage devices. For example, Google stores with the data chunks data indicative of the distinct encryption keys at least by virtue of storing DEKs with the data chunks, and does so on different storage devices. *See supra* at Claim 1[c], 1[d], 1[e]. Google explains that "[e]ach chunk is distributed across our storage systems and is replicated in encrypted form for

backup and disaster recovery." *Id.* Below is an exemplary annotated image from the Google Cloud webpage showing an example of the plurality of different storage devices and data indicative of encryption keys:



80. As a result of Google's infringement of the '854 Patent, SFI has been damaged. SFI is entitled to recover from Google damages sustained as a result of Google's wrongful acts sufficient to compensate SFI for the infringement in an amount subject to proof at trial, and in no event less than a reasonable royalty.

81. To the extent 35 U.S.C. § 287 is determined to be applicable, on information and belief its requirements have been satisfied with respect to the '854 Patent.

82. SFI has suffered and continues to suffer irreparable injury as a direct and proximate result of Google's infringement for which there is no adequate remedy at law. Unless Google is enjoined, SFI will continue to suffer such irreparable injury.

SECOND CLAIM FOR RELIEF

(Infringement of U.S. Patent No. 11,068,609)

83. SFI repeats, re-alleges, and incorporates herein by reference the allegations of Paragraphs 1-82 of its Complaint.

84. On July 20, 2021, United States Patent No. 11,068,609 entitled "Secure Data Parser Method And System" duly and legally issued to inventors Mark S. O'Hare, Rick L. Orsini, Roger S. Davenport, and Steven Winick. On November 22, 2022, the United States Patent Office issued a certificate of correction for the '609 Patent. A true and correct copy of the '609 Patent, together with the certificate of correction, is attached to this Complaint as Exhibit B.

85. SFI is the owner by assignment of the entire right, title, and interest in and to the '609 Patent, including the right to seek damages and any remedies for past, current, and future infringement thereof.

86. The '609 Patent claims priority to United States Provisional Application No. 60/738,231 filed on November 18, 2005.

87. The '609 Patent is valid and enforceable.

88. SFI is informed and believes, and on that basis alleges, that Google has infringed and is currently infringing one or more claims of the '609 Patent, in violation of 35 U.S.C. § 271 *et seq*.

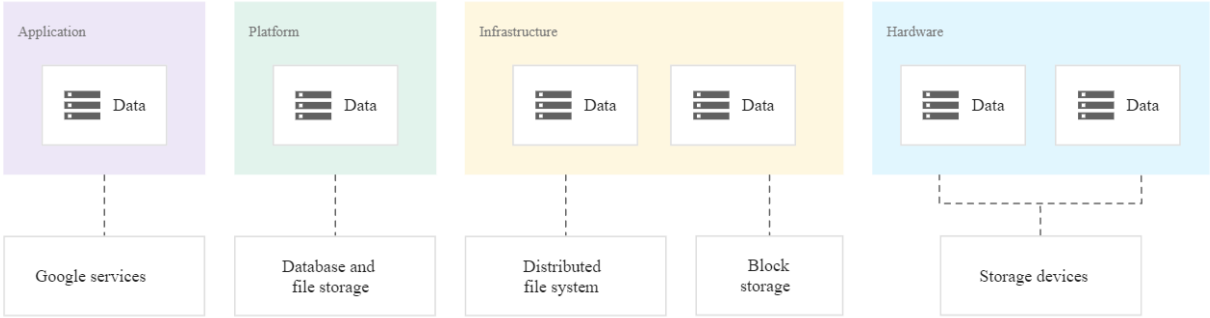
89. Google infringes literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) by, among other things, making, using, offering to sell, and/or selling within this District and elsewhere in the United States, without authority or license, Google products and services falling within the scope of one or more claims of the '609 Patent.

90. For example, as discussed below, the methods and products with which Google performs its encryption technology infringe at least Claim 1 of the '609 Patent.

Claim 1[pre]: A method for securing data, the method comprising:

91. Google meets the preamble (even if the preamble is not limiting). Google securely stores data by, for example, securely storing user data in Google Cloud.

92. For example, Google states its "comprehensive security strategy includes encryption at rest" and it "encrypt[s] all Google customer content at rest, without any action required by [the customer], using one or more encryption mechanisms." Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption. Below is an exemplary image from the Google Cloud webpage showing "the several layers of encryption that are generally used to protect user data in Google production data centers."



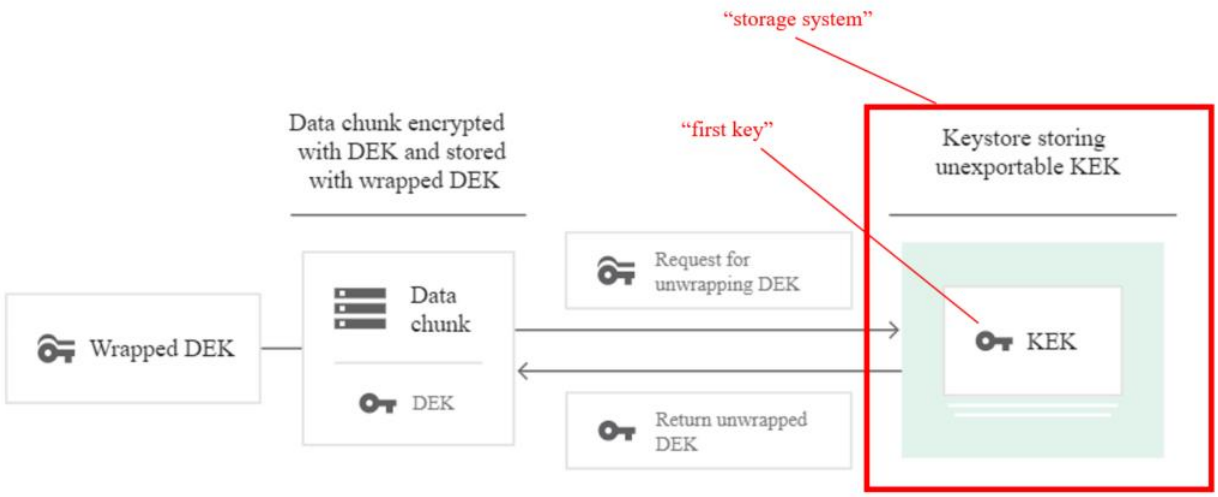
Claim 1[a]: executing code by a processor to perform

93. Google meets this limitation. The Google products and method include executing code by a processor to perform. For example, Google's encryption method requires executing code by a processor such as, for example, the code associated the wrapping and unwrapping keys.

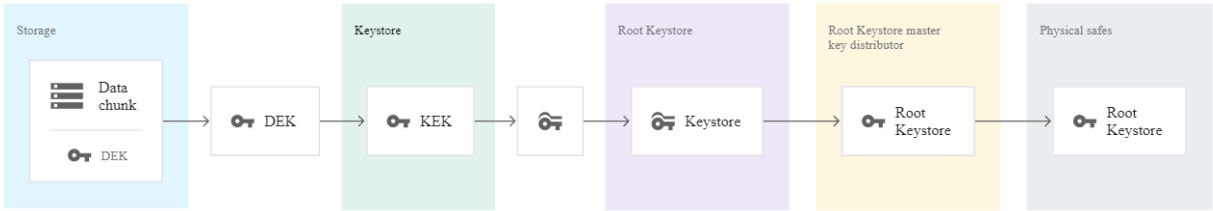
Claim 1[b]: receiving a first key from a storage system,

94. Google meets this limitation. The Google products and method include receiving a first key from a storage system. For example, Google's encryption technology receives a first key from a storage system in the form of, for example, a Key Encryption Key ("KEK") which is

stored in an external storage system Google refers to as "Keystore". *See id*. ("These KEKs are stored centrally in Keystore, a repository built specifically for storing keys."); *id*. ("When a storage system needs to retrieve encrypted data, it retrieves the wrapped DEK and passes it to Keystore. Keystore then verifies that this service is authorized to use the KEK and, if so, unwraps and returns the plaintext DEK to the service."). Below is an exemplary annotated image from the Google Cloud webpage showing an example of a first key from a storage system:

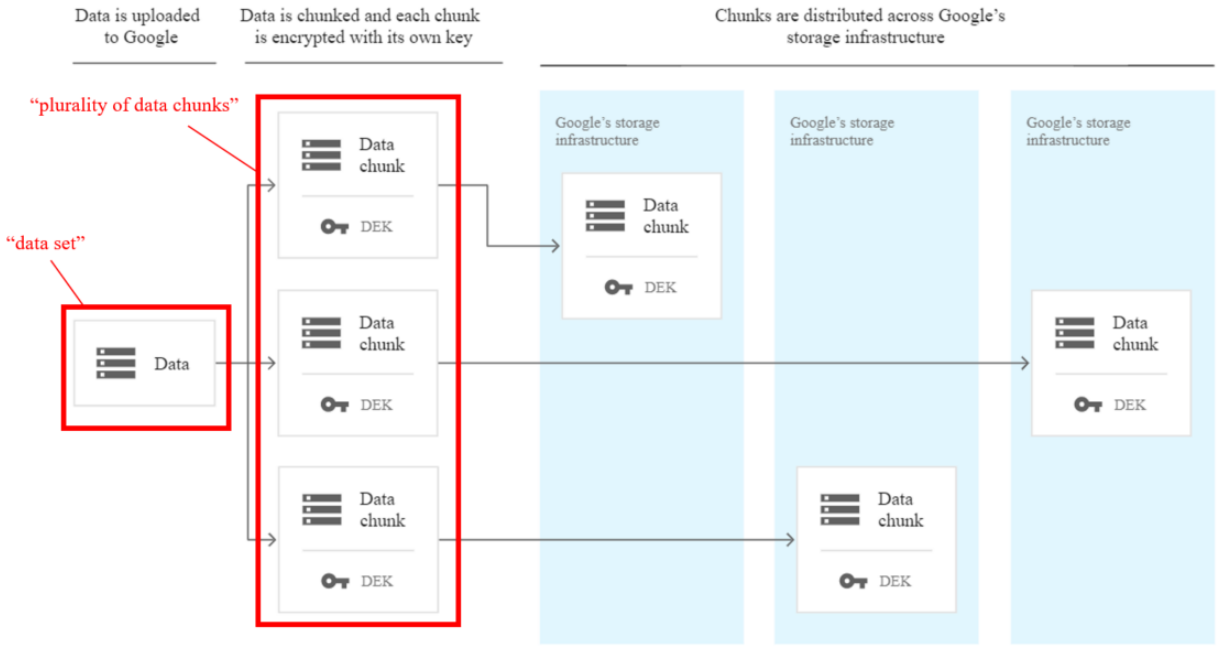


95. This first key is received by, for example, the Root Keystore. Google states that "Keystore is protected by a root key called the *keystore master key*, which wraps all of the KEKs in Keystore. This keystore master key is AES-256 and is itself stored in another key management service, called Root Keystore." *Id*. *See also id*. ("Keystore keys are wrapped with the Keystore master key, which is stored in Root Keystore."). The Root Keystore therefore receives the KEK in order to wrap and return it to Keystore. *See id*:



Claim 1[c]: generating a plurality of data chunks based on a data set, wherein each data chunk of the plurality of data chunks comprises less than an entirety of data of the data set, and wherein the data set can be reconstructed using at least a minimum number of the plurality of chunks;

96. Google meets this limitation. The Google products and method include generating a plurality of data chunks based on a data set, wherein each data chunk of the plurality of data chunks comprises less than an entirety of data of the data set, and wherein the data set can be reconstructed using at least a minimum number of the plurality of chunks. For example, Google generates a plurality of data chunks based on a data set, wherein each data chunk of comprises less than an entirety of data of the data set by splitting a user data set into data chunks. *See id*. ("Data is broken into subfile chunks for storage"). Below is an exemplary annotated image from the Google Cloud webpage showing an example of a data set and plurality of data chunks:



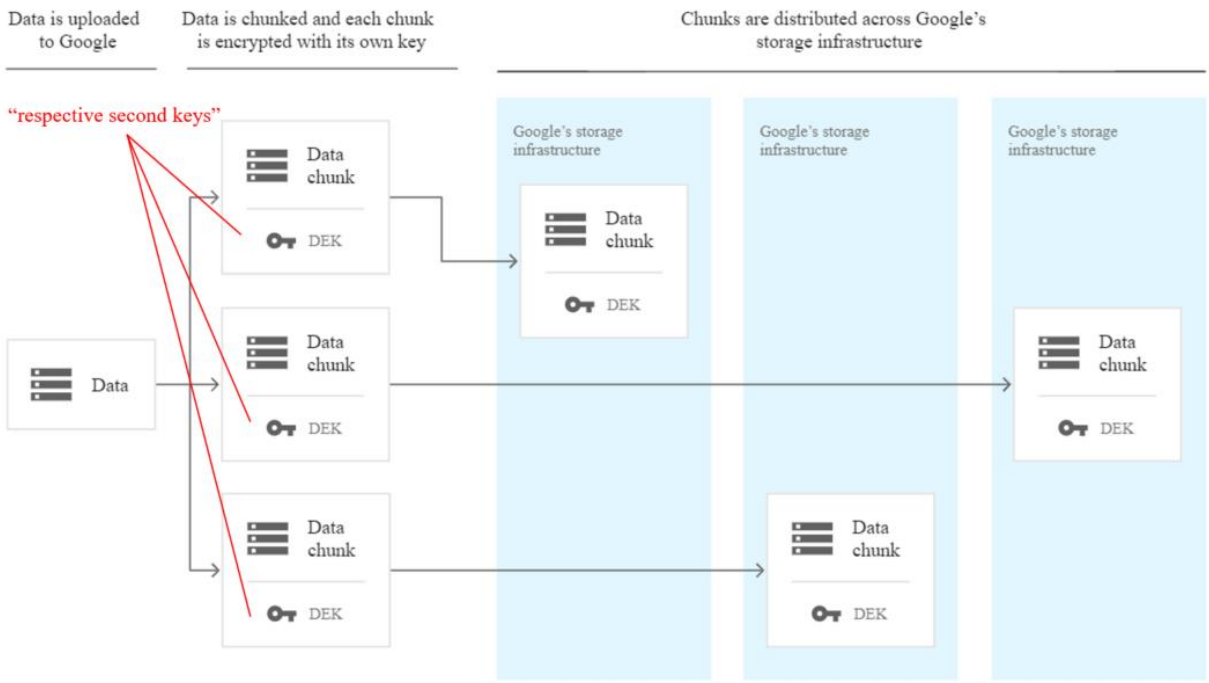
97. As a further example, the data set can be reconstructed using at least a minimum number of the plurality of chunks. Google has explained the operation of this system as follows:

> So first, how does that 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 encryption keys--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 decrypts the data, and sends back the plaintext data to the service, in most cases. In some cases, the service decrypts it directly.

See Kaczorowski, *Managing Encryption of Data in the Cloud* at 8:47-9:59.

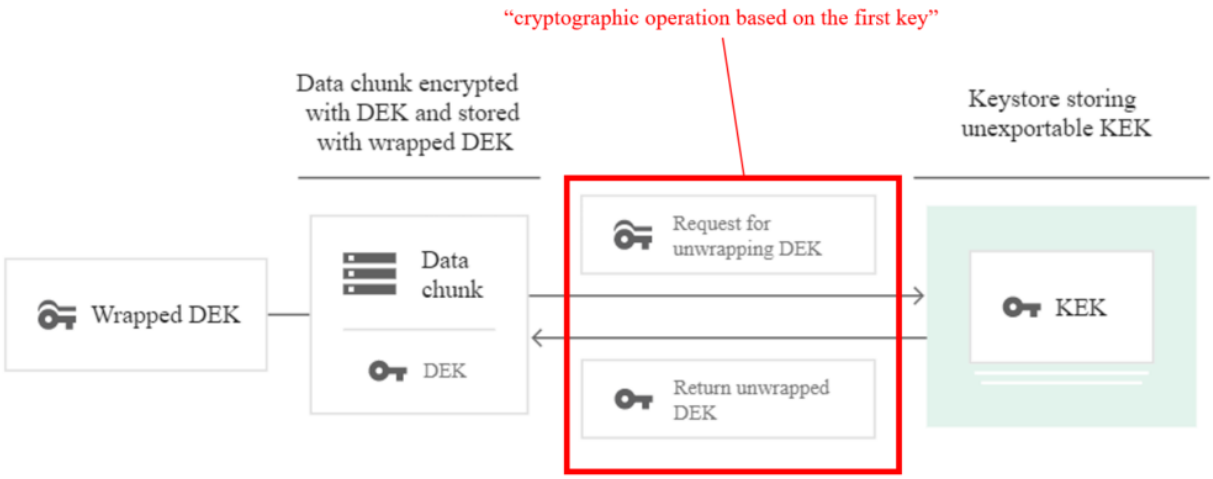
Claim 1[d]: encrypting each respective data chunk of the plurality of data chunks with a respective second key, wherein each of the respective second keys are distinct from each other;

98. Google meets this limitation. The Google products and method include encrypting each respective data chunk of the plurality of data chunks with a respective second key, wherein each of the respective second keys are distinct from each other. For example, Google encrypts each respective data chunk with a distinct second encryption key. 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." *Id*. 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." *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing examples of the respective second keys:



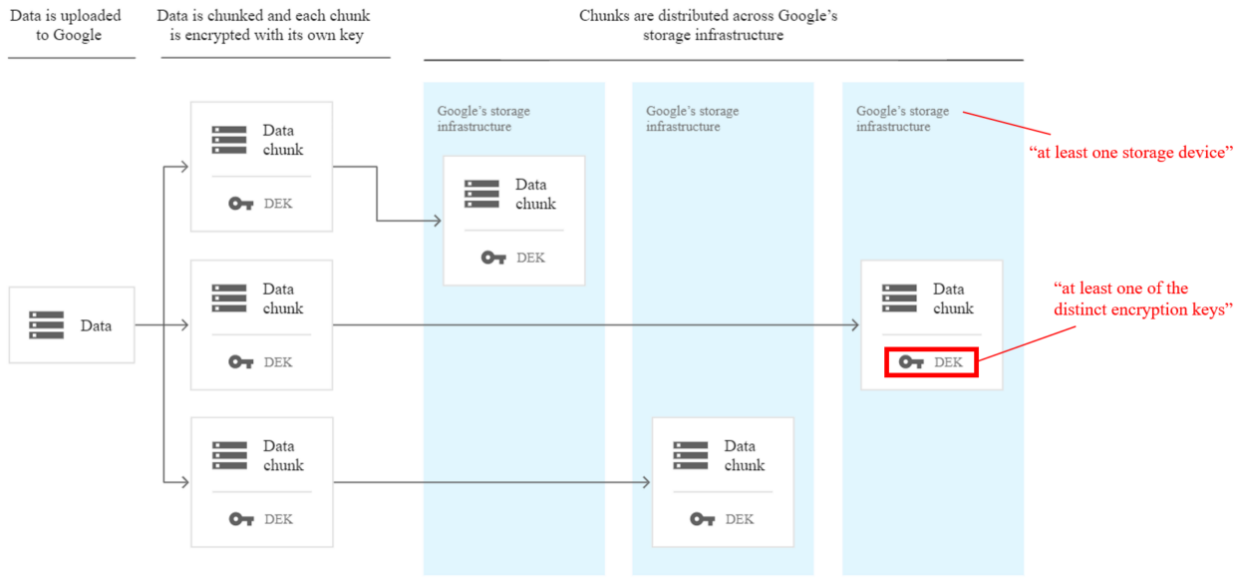
<u>Claim 1[e]: performing a cryptographic operation based on the first key to further secure the plurality of data chunks; and,</u>

99. Google meets this limitation. The Google products and method include performing a cryptographic operation based on the first key to further secure the plurality of data chunks at least because, for example, Google performs encrypts each of the DEKs with a KEK. Google explains that "DEKs are encrypted with (wrapped by) a key encryption key (KEK)." *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing an example of an encryption operation based on the first key:



Claim 1[f]: storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one storage device.

100. Google meets this limitation. The Google products and method include storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one storage device. For example, Google stores, in a memory coupled to a processor, the data chunks with data indicative of at least one of the distinct encryption keys on one or more storage devices at least when it stores DEKs with the data chunks throughout Google's storage infrastructure. *See supra* at Claim 1[c], 1[d]. Google explains that "[e]ach chunk is distributed across our storage systems and is replicated in encrypted form for backup and disaster recovery." *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing an example of the at least one storage device and data indicative of at least one of the distinct encryption keys:



101. As a result of Google's infringement of the '609 Patent, SFI has been damaged. SFI is entitled to recover from Google damages sustained as a result of Google's wrongful acts sufficient to compensate SFI for the infringement in an amount subject to proof at trial, and in no event less than a reasonable royalty.

102. To the extent 35 U.S.C. § 287 is determined to be applicable, on information and belief its requirements have been satisfied with respect to the '609 Patent.

103. SFI has suffered and continues to suffer irreparable injury as a direct and proximate result of Google's infringement for which there is no adequate remedy at law. Unless Google is enjoined, SFI will continue to suffer such irreparable injury.

THIRD CLAIM FOR RELIEF

(Infringement of U.S. Patent No. 11,178,116)

104. SFI repeats, re-alleges, and incorporates herein by reference the allegations of Paragraphs 1-103 of its Complaint.

105. On November 16, 2021, United States Patent No. 11,178,116 entitled "Secure Data Parser Method And System" duly and legally issued to inventors Mark S. O'Hare, Rick L. Orsini,

Roger S. Davenport, and Steven Winick. A true and correct copy of the '116 Patent is attached to this Complaint as Exhibit C.

106. SFI is the owner by assignment of the entire right, title, and interest in and to the '116 Patent, including the right to seek damages and any remedies for past, current, and future infringement thereof.

107. The '116 Patent claims priority to United States Provisional Application No. 60/178,185 filed on September 16, 2005, and United States Provisional Application No. 60/622,146 filed on October 25, 2004.

108. The '116 Patent is valid and enforceable.

109. SFI is informed and believes, and on that basis alleges, that Google has infringed and is currently infringing one or more claims of the '116 Patent, in violation of 35 U.S.C. § 271 *et seq*.

110. Google infringes literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) by, among other things, making, using, offering to sell, and/or selling within this District and elsewhere in the United States, without authority or license, Google products and services falling within the scope of one or more claims of the '116 Patent.

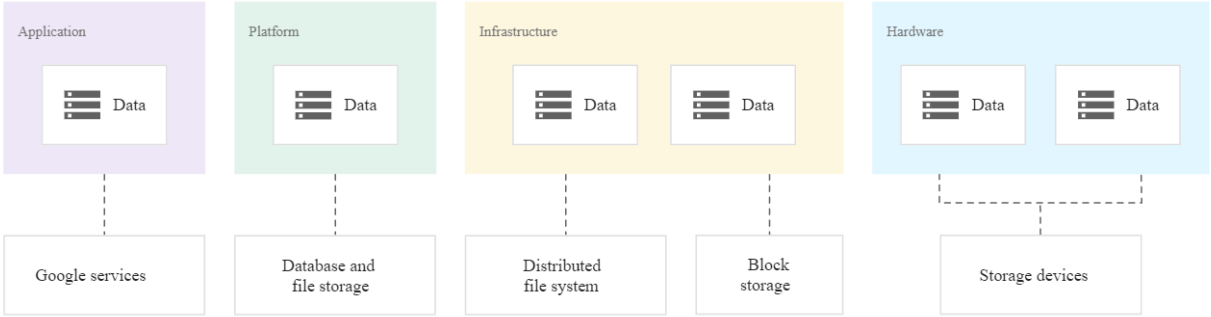
111. For example, as discussed below, the methods and products with which Google performs its encryption technology infringes at least Claim 1 of the '116 Patent.

Claim 1[pre]: A method for securing a data set, the method comprising:

112. Google meets the preamble (even if the preamble is not limiting). Google secures a data set by, for example, securely storing user data in Google Cloud.

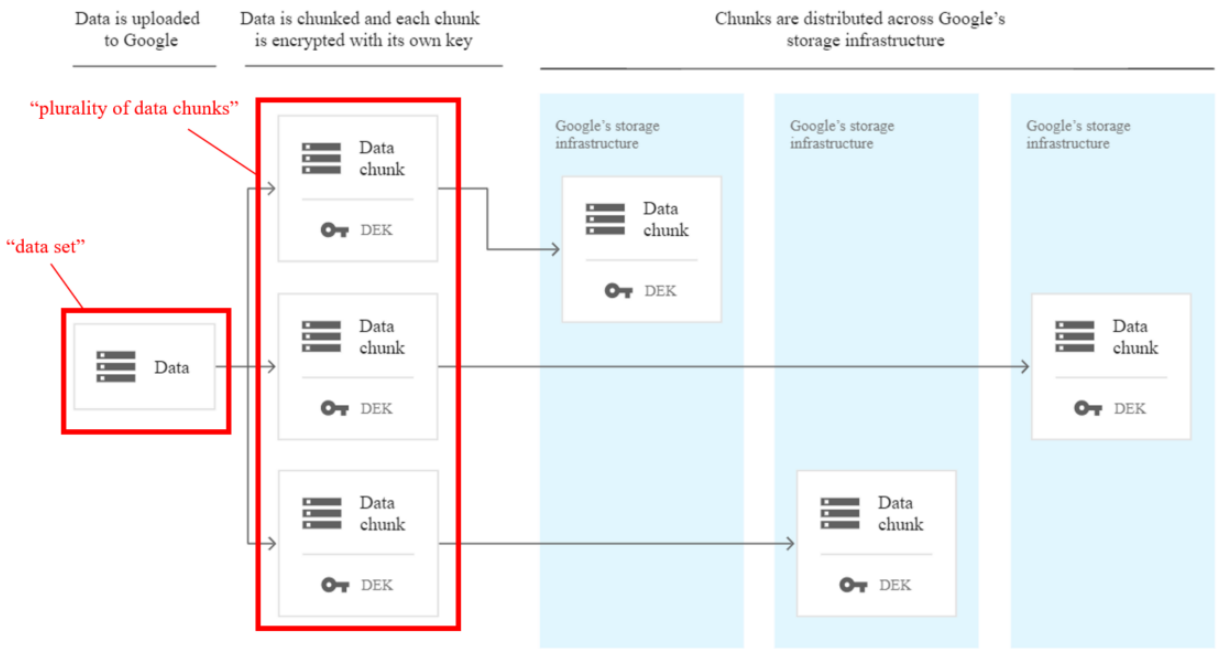
113. For example, Google states its "comprehensive security strategy includes encryption at rest" and it "encrypt[s] all Google customer content at rest, without any action

required by [the customer], using one or more encryption mechanisms." Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption. Below is an exemplary image from the Google Cloud webpage showing "the several layers of encryption that are generally used to protect user data in Google production data centers."



<u>Claim 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;</u>

114. Google meets this limitation. The Google products and method include 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 id*. ("Data is broken into subfile chunks for storage"). Below is an exemplary annotated image from the Google Cloud webpage showing an example of a data set and plurality of data chunks:

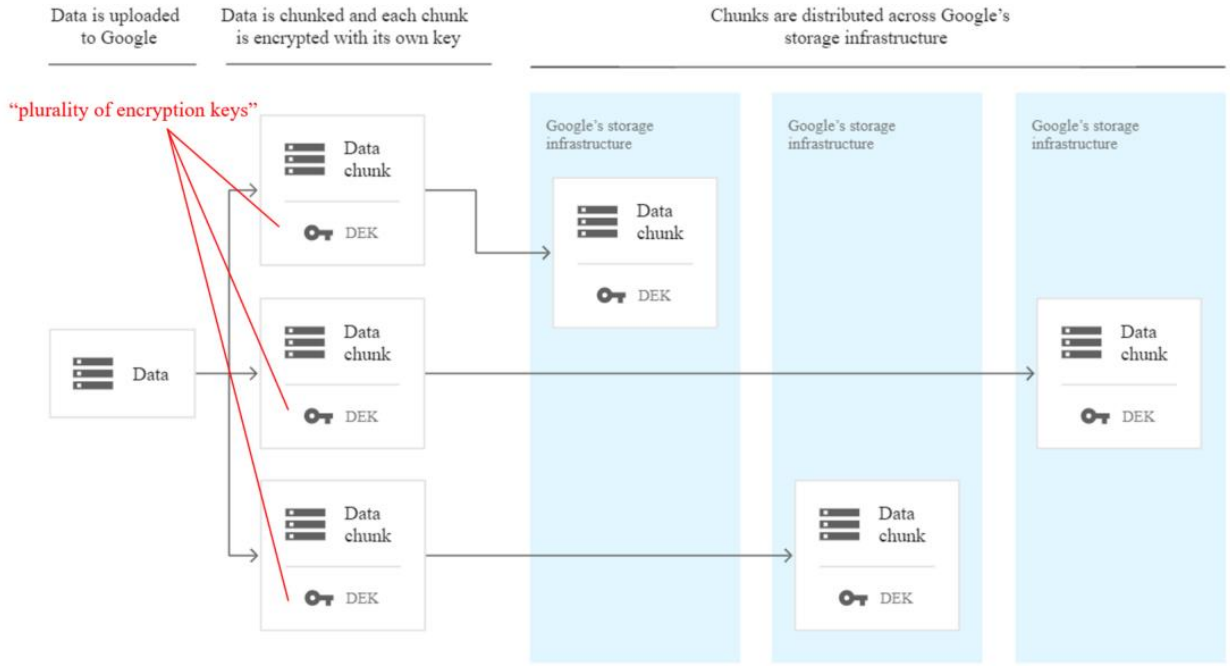


115. Further, none of the data chunks are, by themselves, sufficient to reconstruct the data set. For example, Google explains that "[a]n attacker who wants to access customer data would need to know and be able to access two things: all of the storage chunks that correspond to the data that they want and all of the encryption keys that correspond to the chunks." *Id.*

<u>Claim 1[b]: encrypting each of the data chunks with a respective one of a plurality of encryption keys;</u>

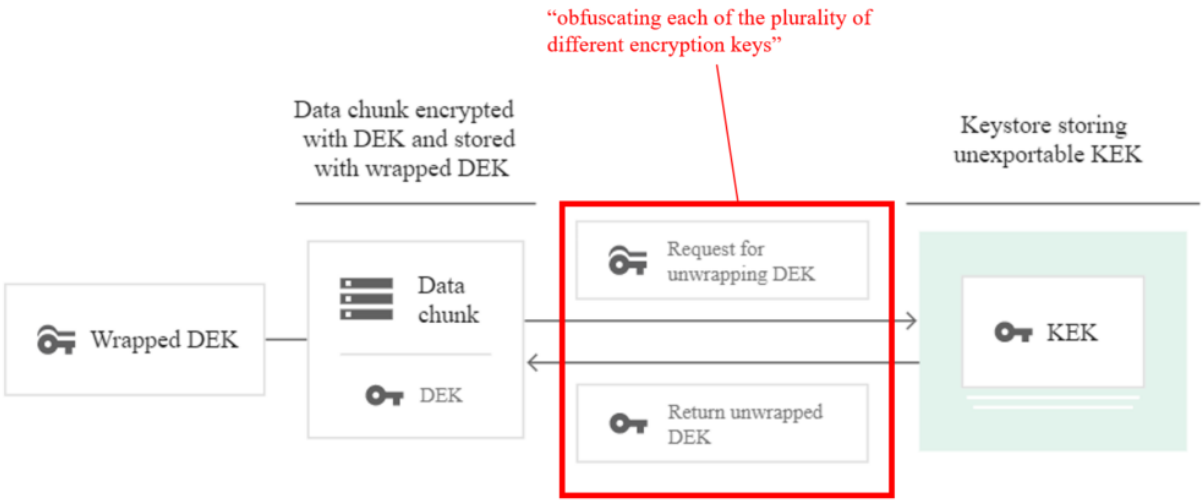
116. Google meets this limitation. The Google products and method include encrypting each of the data chunks with a respective one of a plurality of encryption keys. For example, Google states that "[e]ach chunk is encrypted at the storage level with an individual data encryption key (DEK): two chunks won't have the same DEK, even if they are owned by the same customer or stored on the same machine." *Id.* 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." *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing examples of the plurality of encryption keys:



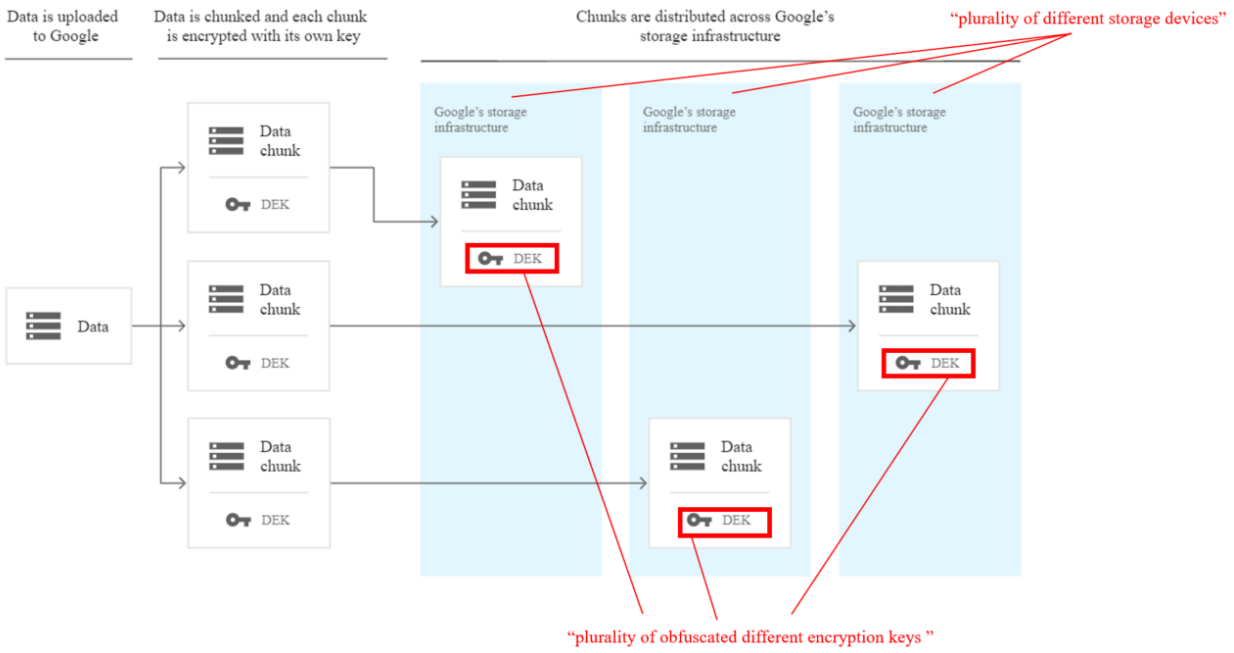
<u>Claim 1[c]: obfuscating each of the plurality of different encryption keys; and</u>

117. Google meets this limitation. The Google products and method include obfuscating each of the plurality of different encryption keys at least because, for example, Google encrypts each of the DEKs with a KEK. Google explains that "DEKs are encrypted with (wrapped by) a key encryption key (KEK)." *Id*. Below is an exemplary annotated image from the Google Cloud webpage showing an example of an encryption operation based on the first key:



Claim 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.

118. Google meets this limitation. The Google products and method include 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, Google stores with the data chunks one of the plurality of obfuscated different encryption keys on a plurality of different storage devices at least by virtue of storing DEKs with the data chunks throughout Google's storage infrastructure. *See supra* at Claim 1[b]. Google explains that "[e]ach chunk is distributed across our storage systems and is replicated in encrypted form for backup and disaster recovery." *Id*. 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:



119. As a result of Google's infringement of the '116 Patent, SFI has been damaged. SFI is entitled to recover from Google damages sustained as a result of Google's wrongful acts sufficient to compensate SFI for the infringement in an amount subject to proof at trial, and in no event less than a reasonable royalty.

120. To the extent 35 U.S.C. § 287 is determined to be applicable, on information and belief its requirements have been satisfied with respect to the '116 Patent.

121. SFI has suffered and continues to suffer irreparable injury as a direct and proximate result of Google's infringement for which there is no adequate remedy at law. Unless Google is enjoined, SFI will continue to suffer such irreparable injury.

FOURTH CLAIM FOR RELIEF

(Infringement of U.S. Patent No. 9,338,140)

122. SFI repeats, re-alleges, and incorporates herein by reference the allegations of Paragraphs 1-121 of its Complaint.

123. On May 10, 2016, United States Patent No. 9,338,140 entitled "Secure Data Parser Method And System" duly and legally issued to inventors Mark S. O'Hare, Rick L. Orsini, Roger S. Davenport, and Steven Winick. A true and correct copy of the '140 Patent is attached to this Complaint as Exhibit D.

124. SFI is the owner by assignment of the entire right, title, and interest in and to the '140 Patent, including the right to seek damages and any remedies for past, current, and future infringement thereof.

125. The '140 Patent claims priority to United States Provisional Application No. 60/178,185 filed on September 16, 2005, and United States Provisional Application No. 60/622,146 filed on October 25, 2004.

126. The '140 Patent is valid and enforceable.

127. SFI is informed and believes, and on that basis alleges, that Google has infringed and is currently infringing one or more claims of the '140 Patent, in violation of 35 U.S.C. § 271 *et seq*.

128. Google infringes literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) by, among other things, making, using, offering to sell, and/or selling within this District and elsewhere in the United States, without authority or license, Google products and services falling within the scope of one or more claims of the '140 Patent.

129. For example, as discussed below, the products and method with which Google performs its encryption technology in connection with Google Drive infringes at least Claim 1 of the '140 Patent.

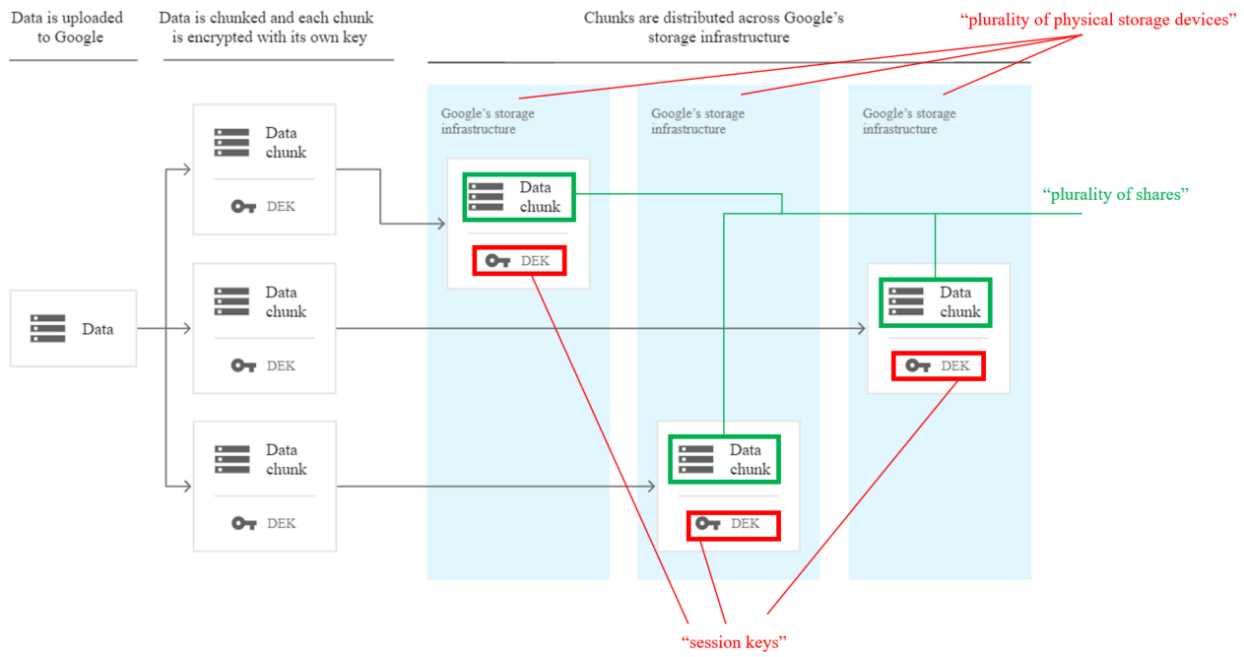
Claim 1[pre]: A secure storage network comprising:

130. Google meets the preamble (even if the preamble is not limiting). For example, Google Drive and its use of encryption technology through Google Cloud are a secure storage network.

131. 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." *How Drive Protects Your Privacy & Keeps You in Control*, Google Drive Help, https://support.google.com/drive/answer/10375054?hl=en (last visited Mar. 10, 2023).

Claim 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

132. Google meets this limitation. The Google secure storage network includes 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 DEK, and each share and DEK are stored on one of a plurality of physical storage devices. *See Default Encryption at Rest: Layers of Encryption*, Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption#layers_of_encryption (last visited Mar. 10, 2023) ("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."). Below is an exemplary annotated image from the Google Cloud webpage showing an example of a plurality of physical storage devices, plurality of shares, and at least one session key used to secure a dataset:



Claim 1[b]: a secure storage system configured to:

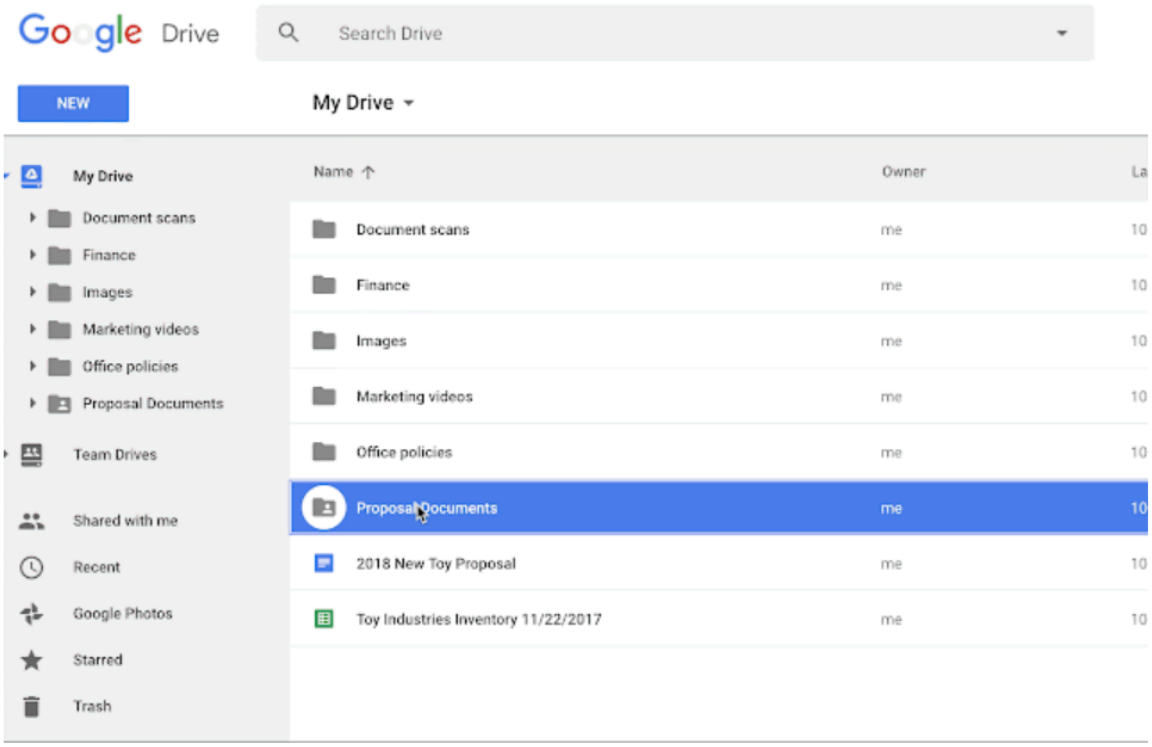
133. Google meets this limitation. For example, Google Drive and its use of encryption technology through Google Cloud comprise a secure storage system.

134. 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." *How Drive Protects Your Privacy & Keeps You in Control*, Google Drive Help, https://support.google.com/drive/answer/10375054?hl=en (last visited Mar. 10, 2023).

Claim 1[c]: 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;

135. Google meets this limitation. The Google secure storage network includes a secure storage system 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. 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*

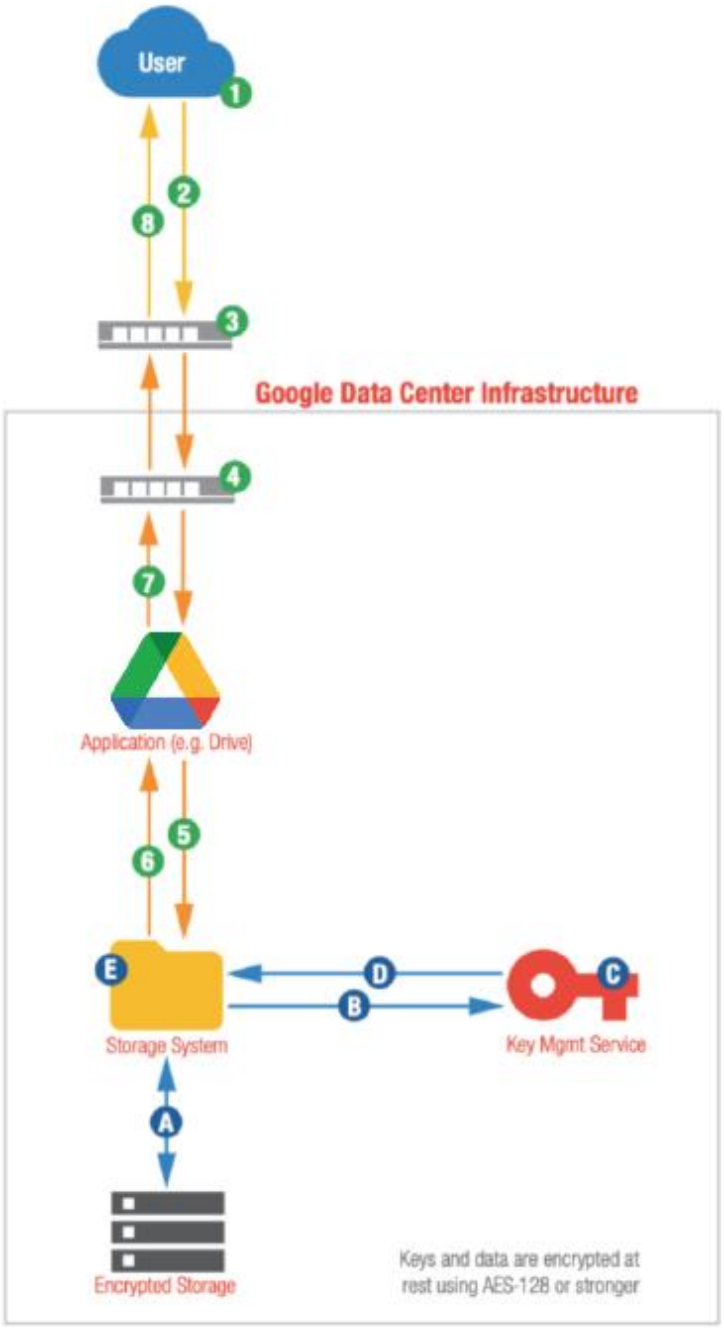
Workspace Updates (Jan. 9, 2018) https://workspaceupdates.googleblog.com/2018/01/search-within-folder-in-google-drive.html:



136. 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 How Google Workspace Uses Encryption to Protect Your Data, Google Cloud Whitepaper* (Aug 2020) https://services.google.com/fh/files/helpcenter/google_encryptionwp2016.pdf:

Encryption at Rest flow

An example of encryption in Google Drive



USER DATA FLOW

1. **Initiate Request**
   User authenticates to Google Workspace and requests Drive data.
2. **Encrypted Tunnel**
   TLS-based encryption dependent on user's browser capabilities.
3. **Google Front End**
   Directs traffic to AFEs.
4. **Application Front End (AFE)**
   Directs traffic to Application servers.
5. **Requests User Data**
   User's Drive data request goes from the Application to storage.
6. **Return Decrypted Data**
   Send user data to Application.
7. **Return User Data**
   Return user data to user.
8. **Return User Data in Encrypted Tunnel**
   Return user data to user.

DATA DECRYPTION

A. **Retrieve Data**
   Gets Encrypted Chunk and Wrapped Key.

B. **Request Key Unwrap**
   Wrapped key is sent to KMS.

C. **ACL Check**
   Is the requester (e.g. Storage System) authorized to have key unwrapped?

D. **Send Unwrapped Key**
   KMS unwraps the encryption key data, which Storage System will use to decrypt chunk.

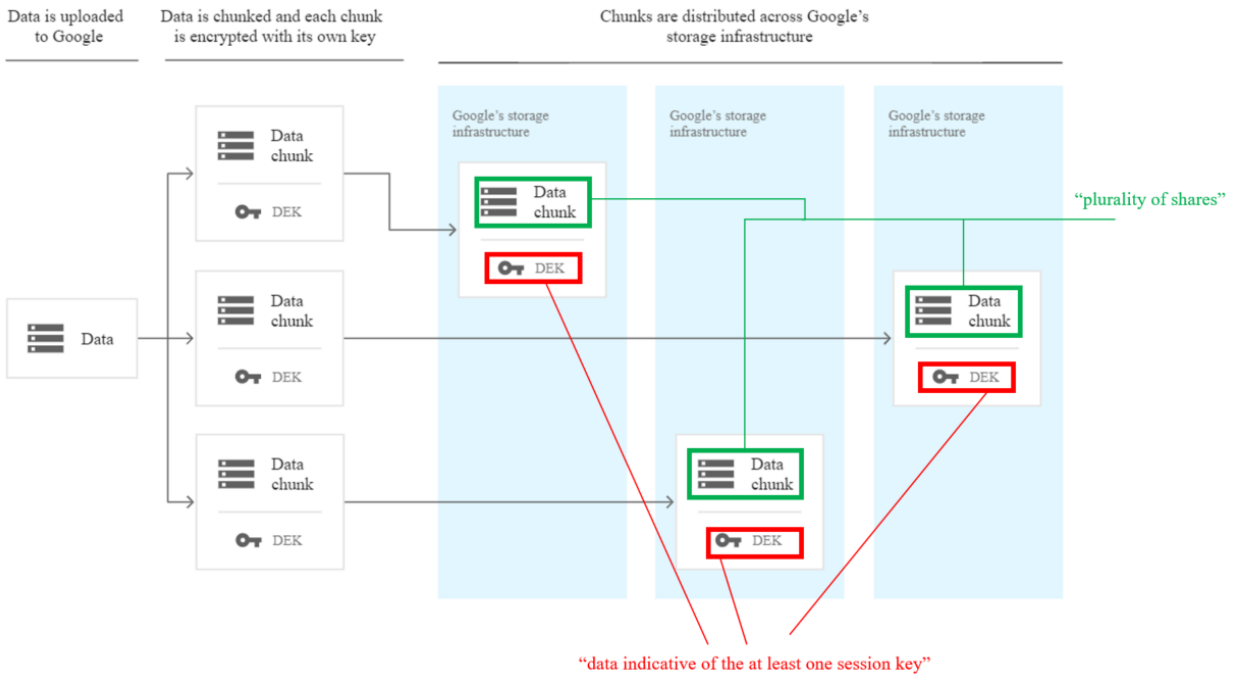
E. **Decrypt Data**
   Storage System decrypts chunk.

Claim 1[d]: 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;

137. Google meets this limitation. The Google secure storage network includes 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)." Google Cloud, https://cloud.google.com/docs/security/encryption/default-encryption#layers_of_encryption. 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." *Id*. Below is an exemplary image from the Google Cloud webpage showing how data is "chunked" and "encrypted":

<u>Claim 1[e]: include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset; and</u>

138. Google meets this limitation. The Google secure storage network includes 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 at least because, 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 chunks. *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:



Claim 1[f]: 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.

139. Google meets this limitation. The Google secure storage network includes 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. For example, Google has explained the operation of this system as follows:

> So first, how does that 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 encryption keys--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 decrypts the data, and

> sends back the plaintext data to the service, in most cases. In some cases, the service decrypts it directly.

See Kaczorowski, *Managing Encryption of Data in the Cloud* at 8:47-9:59.

140. As a result of Google's infringement of the '116 Patent, SFI has been damaged. SFI is entitled to recover from Google damages sustained as a result of Google's wrongful acts sufficient to compensate SFI for the infringement in an amount subject to proof at trial, and in no event less than a reasonable royalty.

141. To the extent 35 U.S.C. § 287 is determined to be applicable, on information and belief its requirements have been satisfied with respect to the '116 Patent.

142. SFI has suffered and continues to suffer irreparable injury as a direct and proximate result of Google's infringement for which there is no adequate remedy at law. Unless Google is enjoined, SFI will continue to suffer such irreparable injury.

PRAYER FOR RELIEF

WHEREFORE, SFI prays for judgment against Google as follows:

A. That Google has infringed, and unless enjoined will continue to infringe, each of the Asserted Patents;

B. That Google pay SFI damages adequate to compensate SFI for Google's infringement of each of the Asserted Patents, together with interest and costs under 35 U.S.C. § 284;

C. That Google be ordered to pay prejudgment and post-judgment interest on the damages assessed;

D. That Google be ordered to pay supplemental damages to SFI, including interest, with an accounting, as needed;

E. That Google be enjoined from infringing the Asserted Patents, or if its infringement is not enjoined, that Google be ordered to pay ongoing royalties to SFI for any post-judgment infringement of the Asserted Patents;

F. That this is an exceptional case under 35 U.S.C. § 285, and that Google pay SFI's attorneys' fees and costs in this action; and

G. That SFI be awarded such other and further relief, including equitable relief, as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), SFI hereby demands a trial by jury on all issues so triable.

Dated: March 10, 2023

By: */s/ Charles B. Molster, III*

Charles B. Molster, III
Virginia Bar No. 23613
The Law Offices of Charles B. Molster, III PLLC
2141 Wisconsin Avenue, N.W., Suite M
Washington, D.C. 20007
Telephone: (202) 787-1312
Cell: (703) 346-1505
cmolster@molsterlaw.com

Andrei Iancu (*pro hac vice* to be filed)

IRELL & MANELLA LLP
750 17th Street NW, Suite 850
Washington, DC 20006
Telephone: (202) 777-6500
aiancu@irell.com

Jonathan Lindsay (*pro hac vice* to be filed)

IRELL & MANELLA LLP

840 Newport Center Drive, Suite 400
Newport Beach, California 92660
Telephone: (949) 760-0991
Facsimile: (949) 760-5200
jlindsay@irell.com

Jordan Nafekh (*pro hac vice* to be filed)
Erick Franklund (*pro hac vice* to be filed)

IRELL & MANELLA LLP
1800 Avenue of the Stars, Suite 900
Los Angeles, California 90067
Telephone: (310) 277-1010
Facsimile: (310) 203-7199
jnafekh@irell.com
efranklund@irell.com

Attorneys for Plaintiff Security First Innovations, LLC