

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

SECURITY FIRST INNOVATIONS, LLC,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Civil Action No. 2:23-cv-00097 (JKW-RJK)

**GOOGLE LLC'S OPENING CLAIM
CONSTRUCTION BRIEF**

TABLE OF CONTENTS

	<u>Page</u>
Background	1
Legal Standard	2
Argument	4
I. Distributing / Generating Data Chunks or Shares (<i>All Claims</i>).....	4
A. Distributing the Data Set into Chunks or Shares	5
B. Generating a Plurality of Data Chunks	7
II. Data Indicative of ... Key(s) (' <i>140 cl. 1</i> ; ' <i>854 cl. 1</i> ; ' <i>609 cl. 1, 2, 3</i>).....	9
A. Google's Construction is Supported by The Intrinsic Evidence and Plain Meaning of the Phrase at issue	10
B. SFI's Construction Is Not Supported By The Intrinsic Evidence And Does Not Aid The Fact Finder.....	12
III. Dataset / Data Set (<i>All Claims</i>).....	14
A. The Intrinsic Evidence Consistently Refers to a "Data Set" as a Unit	14
B. The Extrinsic Evidence Further Supports Google's Construction.....	15
IV. Data Set / The Data Set.....	16
V. Virtual Disk [] Comprising a Directory Mapped to the Plurality of Physical Storage Devices (' <i>140 cl. 1</i>).....	17
VI. External Key (' <i>854 cl. 1</i>)	20
VII. Minimum Number of the Plurality of [Data] Chunks (' <i>854 cl. 1</i> ; ' <i>609 cl. 1</i>).....	22
VIII. Separately Storing Each Data Chunk of the Plurality of Data Chunks Together with One of the Plurality of Obfuscated Different Encryption Keys (' <i>116 cl. 1</i>).....	25
A. The Intrinsic Evidence Supports Google's Proposal	25
B. SFI's Proposal Is Untethered from the Teachings of the Patents	26
IX. Transforming / Performing a Transform (' <i>116 cl. 2, 9</i>).....	27
X. Session Key (' <i>140 cl. 1, 8</i>).....	30

TABLE OF AUTHORITIES

	<u>Page(s)</u>
<u>Cases</u>	
<i>Bicon, Inc. v. Straumann Co.</i> , 441 F.3d 945 (Fed. Cir. 2006).....	12, 13, 14, 24
<i>C.R. Bard, Inc. v. U.S. Surgical Corp.</i> , 388 F.3d 858 (Fed. Cir. 2004).....	23
<i>Cybergym Rsch. LLC v. Icon Health & Fitness, Inc.</i> , 2007 WL 5688735 (E.D. Tex. Jan. 25, 2007).....	17
<i>Eon Corp. IP Holdings v. Silver Spring Networks</i> , 815 F.3d 1314 (Fed. Cir. 2016).....	8, 24
<i>GPNE Corp. v. Apple Inc.</i> , 830 F.3d 1365 (Fed. Cir. 2016).....	8, 10, 24, 26, 29
<i>Honeywell Int'l, Inc. v. Int'l Trade Comm'n</i> , 341 F.3d 1332 (Fed. Cir. 2003).....	27
<i>Infernal Tech., LLC v. Activision Blizzard Inc.</i> , No. 2021-2349, 2023 WL 370602 (Fed. Cir. Jan. 24, 2023)	16, 17
<i>Intel Corp. v. Qualcomm Inc.</i> , 21 F.4th 801 (Fed. Cir. 2021)	11
<i>Interval Licensing LLC v. AOL, Inc.</i> , 766 F.3d 1364 (Fed. Cir. 2014).....	27, 29
<i>Markman v. Westview Instruments, Inc.</i> , 517 U.S. 370 (1996).....	2, 3
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014).....	3, 4, 12, 13, 27, 29
<i>Nystrom v. TREX Co.</i> , 424 F.3d 1136 (Fed. Cir. 2005).....	8, 18, 24
<i>O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.</i> , 521 F.3d 1351 (Fed. Cir. 2008).....	4, 17, 21
<i>Oasis Rsch., LLC v. AT&T Corp.</i> , 2012 WL 602199 (E.D. Tex. Feb. 23, 2012)	19

<i>In re Packard</i> , 751 F.3d 1307 (Fed. Cir. 2014).....	4
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005).....	1, 3, 6, 7, 13, 19, 22, 27
<i>Process Control Corp. v. HydReclaim Corp.</i> , 190 F.3d 1350 (Fed. Cir. 1999).....	16
<i>SFA Sys., LLC v. 1-800-Flowers.com, Inc.</i> , 940 F. Supp. 2d 433 (E.D. Tex. 2013).....	17
<i>Trustees of Columbia Univ. in City of New York v. NortonLifeLock, Inc.</i> , No. 3:13CV808, 2019 WL 7040931 (E.D. Va. Dec. 20, 2019).....	9
<i>Verizon Servs. Corp. v. Vonage Holdings Corp.</i> , 503 F.3d 1295 (Fed. Cir. 2007).....	7, 23
<i>Warner–Lambert Co. v. Apotex Corp.</i> , 316 F.3d 1348 (Fed. Cir. 2003).....	16
<i>Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.</i> , 853 F.3d 1272 (Fed. Cir. 2017).....	12, 24
<i>Wisconsin Alumni Rsch. Found. v. Apple Inc.</i> , 905 F.3d 1341 (Fed. Cir. 2018).....	8, 24

Statutes

35 U.S.C. § 112.....	3
----------------------	---

Other Authorities

Mann, Charles C., <i>A Primer on Public-key Encryption</i> , THE ATLANTIC, p. 6 (Sept. 2002 issue).....	30
<i>The Microsoft Computer Dictionary</i> , 4th Ed. (1999)	15, 18
<i>The Microsoft Computer Dictionary</i> , 5th Ed. (2002)	15, 29, 30
<i>Newton’s Telecom Dictionary</i> , 16th Ed. (2000)	18, 30
<i>Oxford English Dictionary</i> , 2d Ed. (1994).....	11, 12, 22, 26, 27
Rivest, Ronald L., <i>All-Or-Nothing Encryption and The Package Transform</i> , 1997	28
U.S. Patent No. 9,338,140.....	2, 14, 17, 18, 19
U.S. Patent No. 9,992,170.....	11, 12

U.S. Patent No. 10,108,807.....	11
U.S. Patent No. 10,452,854.....	2, 5, 6, 7, 20, 21, 22, 23
U.S. Patent No. 11,068,609.....	1, 2, 5, 7
U.S. Patent No. 11,178,116.....	2, 24, 25, 27, 28
<i>Webster's Third New Int'l Dictionary</i> (2002).....	11, 26, 29

NOTE ON CITATIONS

- The patents-in-suit, 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”); are attached as Exhibits A through D, respectively. References to the patents-in-suit are listed by column and line number, or by claim number. The ’140 and ’116 patents share the same specification, as do the ’854 and ’609 patents. Further, the four patents share the same first 35 figures and corresponding 75 columns of text. (The different material begins at Col. 76, line 4 of the ’140 patent, and at Col. 77, line 27 of the ’854 patent.)
- All references are to the ’140 patent unless otherwise stated. Such references also encompass the corresponding language in the ’116 patent and– when within the first 75 columns of text– the corresponding language in the ’854 and ’609 patents. For example, “11:18-30” refers to Column 11, lines 18-30 of the ’140 patent; as well as Column 11, lines 42-54 of the ’116 patent; Column 11, lines 5-17 of the ’854 patent; and Column 11, lines 5-17 of the ’609 patent.
- References to claims in the patents-in-suit are cited by the shortened patent number followed by “cl.” and the claim number. For example, “’140 cl. 1” refers to claim 1 of the ’140 patent.
- “Compl.” refers to SFI’s Complaint filed in this action (Dkt. 1).
- “Webster’s Int’l Dictionary” refers to *Webster’s Third New Int’l Dictionary* (2002), excerpts of which are attached as Exhibit E.
- “Newton’s Dictionary” refers to *Newton’s Telecom Dictionary*, 16th Ed. (2000), excerpts of which are attached as Exhibit F.

- “Microsoft 4th Dictionary” refers to *The Microsoft Computer Dictionary*, 4th Ed. (1999), excerpts of which are attached as Exhibit G.
- “Microsoft 5th Dictionary” refers to *The Microsoft Computer Dictionary* (5th ed. 2002), excerpts of which are attached as Exhibit H.
- “American Dictionary” refers to *The American Heritage College Dictionary*, 4th Ed. (2002), excerpts of which are attached as Exhibit I.
- “Oxford Dictionary” refers to *Oxford English Dictionary* (2d ed. 1994), excerpts of which are attached as Exhibit J.
- “SFI Evidence” refers to the November 10, 2023 Letter from A. Mayron to D. Perlson, which is attached as Ex. K.
- Emphasis in brief added unless otherwise noted.

As explained herein, Google construes terms according to their meaning in light of the claims and specification as required by the Federal Circuit’s seminal, *en banc* decision in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). In contrast, SFI offers “no construction necessary” for all but two terms. The constructions SFI does provide are either cherry-picked, in whole or part, from dictionaries, taken from case law concerning other patents with different specifications, or simply divorced from the patents and its own proffered extrinsic evidence. This is the very approach the Federal Circuit has consistently found improper. Google’s constructions should be adopted.

Background

Each Accused Patent is titled “Secure Data Parser Method and System.” As the patents acknowledge, using encryption to secure and/or verify access to data was well known, and “any encryption process is suitable for use in the process of the present invention.” 1:38-49, 53:6-9. Similarly, the claimed inventions purportedly encompass “a wide number of alternatives for the data splitting process The data may be split into any desired, selected, predetermined, or randomly assigned size unit, including but not limited to, a bit, bits, bytes, kilobytes, megabytes or larger, or any combination or sequence of sizes.” 21:13-40. In denying Google’s Motion to Dismiss under Section 101, the Court found “[t]he ‘purportedly innovative technological solution’ of these claims is rooted in the particular sequence of parsing, encrypting, and storing steps they describe.” Dkt. 125 at 44.

Exemplary claim 1 of the ’609 patent is reproduced below:

1. A method for securing data, the method comprising:

executing code by a processor to perform:

receiving a first key from a storage system;

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;

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;

performing a cryptographic operation based on the first key to further secure the plurality of data chunks; and

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.

As the Court stated, '609 claim 1 "requires parsing data into chunks, encrypting those chunks with different encryption keys, further encrypting the chunks with another key, and storing each chunk with data indicative of a key on a storage device." Dkt. 125 at 40.

The remaining patents recite similar requirements and also require that "chunks of data . . . be stored on more than one storage device." *Id.* at 41. Claim 1 of the '854 patent also "further secure[s]" the encrypted data chunks via an "encryption operation" that uses an "external key," rather than via a "cryptographic operation" that uses a "first key." Claim 1 of the '116 patent replaces the "cryptographic operation" of the '609 patent with "obfuscating" the encryption keys, while claim 9 of the same patent instead "transforms" the encryption keys. Claim 1 of the '140 patent drops the "encryption operation" altogether and instead presents a "virtual disk" by which a client device can access and retrieve the stored encrypted data. As the Court found in denying Google's Motion to Dismiss, "any method of 'parsing and encrypting stored data' that does not utilize the claimed virtual disk is outside the scope of the claim." *Id.*

Legal Standard

In *Markman v. Westview Instruments, Inc.*, 517 U.S. 370 (1996), the Supreme Court explained the basis and importance of claim construction. "Victory in an infringement suit requires

a finding that the patent claim covers the alleged infringer's product or process, which in turn necessitates a determination of what the words in the claim mean." *Id.* at 374 (internal quotation marks and citation omitted). Determining the proper interpretation of disputed claim terms "is an issue for the judge, not the jury." *Id.* at 391.

"The words of a claim 'are generally given their ordinary and customary meaning,'" which is their meaning to a "person of ordinary skill in the art [(‘POSITA’)] in question at the time of the invention" "after reading the entire patent." *Phillips*, 415 F.3d at 1312-17, 1321. While it is a "bedrock principle" of patent law that "the claims of a patent define the invention," the specification of a patent "is always highly relevant to the claim construction analysis" and "is the single best guide to the meaning of a disputed term." *Id.*, 1312, 1315. "[A] [C]ourt 'should also consider the patent's prosecution history.'" *Id.*, 1317. As with the specification, "the prosecution history provides evidence of how the PTO and the inventor understood the patent," and can reveal "whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be." *Id.* The claims, specification and file history are called "intrinsic evidence," and are of paramount importance. *Id.*, 1314-17.

The Court also may consult "extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." *Id.*, 1314. Extrinsic evidence includes "expert and inventor testimony, dictionaries, and learned treatises." *Id.*, 1317. "[W]hile extrinsic evidence can shed useful light on the relevant art, [] it is less significant than the intrinsic record in determining the legally operative meaning of claim language." *Id.* (cleaned up). Under 35 U.S.C. § 112, ¶ 2, the claims must "particularly point[] out and distinctly claim[] the subject matter which the inventor or a joint inventor regards as the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). Claims must define the scope of the invention with "reasonable

certainty” and provide “clear notice” of what is claimed, “appris[ing] the public of what is still open to them.” *Id.* at 901, 909-10. Indefiniteness renders a claim invalid, and the Court may not rewrite claims to preserve their validity. *Id.* at 902. Indefiniteness is considered as a matter of law as part of claim construction. *In re Packard*, 751 F.3d 1307, 1311 (Fed. Cir. 2014).

“A determination that a claim term ‘needs no construction’ or has the ‘plain and ordinary meaning’ may be inadequate when a term has more than one ‘ordinary’ meaning or when reliance on a term’s ‘ordinary’ meaning does not resolve the parties’ dispute.” *O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1361 (Fed. Cir. 2008). That is because “[w]hen the parties present a fundamental dispute regarding the scope of a claim term, it is the court’s duty to resolve it.” *Id.* at 1362. It is thus improper to submit the parties’ arguments regarding the meaning and legal significance of a claim limitation to the jury. *Id.* SFI’s expected arguments, based on the parties’ claim construction meet and confer, that no construction is necessary because the jury will simply “understand” the meaning of the various terms is contrary to black letter law. Where the parties dispute the meaning of a phrase, it is for the Court, not the jury, to resolve.

Argument¹

I. DISTRIBUTING / GENERATING DATA CHUNKS OR SHARES (ALL CLAIMS)

As the Court noted in reference to all asserted claims, “[a]t a high level, the claims are directed to a method for securing data that involves splitting data, encrypting the data with encryption keys, and storing the data and the encryption keys in one or more places.” Dkt. 125 at 2. The claims use two sets of related verbiage to recite the “splitting” portion: they either “distribut[e] the data set into a plurality of shares” or “chunks” (*e.g.*, ’854 claim 1), or they “generat[e] a plurality of data chunks based on a data set.” (*e.g.*, ’609 claim 1). The parties dispute

¹ Google does not believe that any expert testimony is necessary for any disputed claim term that has been briefed herein.

whether the data set is “split” into shares or chunks consistent with the intrinsic evidence as the Court already found (Google), or whether the claims require “dividing *and* placing” the data set into shares or chunks or “creating” chunks (SFI). The dispute is material, and thus requires resolution, because the accused Google products do not split (or divide) data from data sets into chunks or shares. Instead, data from an incoming data stream goes into a buffer, that once filled, is then encrypted and stored.

A. DISTRIBUTING THE DATA SET INTO CHUNKS OR SHARES

Google: “splitting the data set into a plurality of data chunks” (’116 claim 1, 9) “splitting the data set into a plurality of shares” (’854 claim 1) “splitting the data set into shares” (’140 claim 1)	SFI: No construction necessary In the alternative: “dividing and placing the data set into a plurality of [data chunks/the shares/a plurality of shares]” (’854 claim 1; ’116 claims 1, 9; ’140 claim 1)
--	--

The ’854 patent recites “distributing the data set into a plurality of shares,” and the ’116 and ’140 patents recite similar language. At first blush, the parties’ constructions for the “distributing” language are similar, with Google proposing “splitting” and SFI proposing “dividing and placing.”

Google’s construction more closely tracks the specification, which repeatedly states that data sets are “split” into chunks or shares. *See, e.g.*, Abstract (“The secure data parser parses data and then splits the data into multiple portions that are stored or communicated distinctly.”), 2:33-37 (“The method comprises one or more steps of parsing, splitting and/or separating the data to be secured into two or more parts or portions.”), 15:32-40, 18:15-48, 20:18-21:40, 52:55-55:55, Figs. 5, 6, 21-24. It also tracks how the Court and SFI have characterized the patents as requiring “splitting.” Dkt. 125 at 2 (quoted *supra*), 11 (quoting SFI as stating that “the method that SFC had invented to secure cloud-based data that comprised splitting the data into chunks...”), 19 (same), 42 (“The specification of the ’609 patent also describes the advantages of splitting the chunks of parsed, encrypted data onto different storage devices...”); Compl. ¶¶ 15 (“The Asserted Patents

focus on solving those inadequacies by, among other things, unconventionally parsing and splitting the data into different portions before storage.”), 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...”), 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.”); 27 (“[T]he 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.”).

In contrast, SFI’s alternative proposal appears to have been lifted from a dictionary for the word “distributing.” SFI Evidence (relying on a dictionary for “distribute” as “[t]o divide and place into classes, or other divisions”). But such extrinsic evidence should not be given weight over the intrinsic evidential support for Google’s construction. *Phillips*, 415 F.3d at 1324 (extrinsic evidence may not be “used to contradict claim meaning that is unambiguous in light of the intrinsic evidence”). While “dividing” is likely a synonym for “splitting,” Google submits that it is better to use the “splitting” language given the Court’s rulings and patents’ disclosures. Indeed, at the parties’ meet and confer, SFI could not articulate any basis for why it would not agree to the “splitting” language given the Court’s 101 Order in particular. If SFI wants to deviate from the language that its patents use to describe the distributing (and generating) step, SFI should be able to explain why that is appropriate or needed. SFI has not, leaving the inference it will later argue dividing means something other than the “splitting” to which the intrinsic evidence consistently refers to, as SFI itself previously acknowledged.

Moreover, SFI is not just avoiding “splitting” with no explanation; it is attempting to include a requirement that this term requires “dividing *and placing*.” There is no support for that

interpretation in the specification. Instead, the patents repeatedly explain that the shares or chunks are the result of splitting (e.g., dividing) the data set. *See supra*. The patents do not require an additional “placing” step, and it is unclear what that would even refer to in the context of the claims and specifications.² Google’s proposal should be adopted.

B. GENERATING A PLURALITY OF DATA CHUNKS

Google: “splitting the data set into a plurality of data chunks” (’609 claim 1)	SFI: No construction necessary; In the alternative: “creating a plurality of data chunks based on [a/the] data set” (’609 claim 1)
--	--

The ’609 patent recites “generating a plurality of data chunks based on a data set.” As noted above, it is black-letter law of claim construction that “the specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; *it is the single best guide to the meaning of a disputed term.*” *Phillips*, 415 F. 3d at 1315 (cleaned up, emphasis added). Here, the specification consistently and exclusively explains that in the “present invention,” the data set is split into “chunks” or “shares,” which is what it means to “generate” the “chunks” or “shares.” Abstract (“The secure data parser parses data and then splits the data into multiple portions that are stored or communicated distinctly.”), 67:34-57 (“Message 2704 is parsed and split by secure data parser 2702 *in accordance with the present invention*”); 71:42-45 (“Secure data processor 3000 then parses and splits the data it takes as input from assembled data buffer 3008 *in accordance with the present invention*”); *see also* 20-30, 6:41-45, 8:15-22, 8:39-41, 18:15-31, 21:13-40, 52:55-53:5, 53:40-55:47, 67:58-68:11, Figs. 6, 37-39, 46; ’854 patent at 77:43-57. “When a patent thus describes the features of the ‘present invention’ as a whole, this description limits the scope of the invention.” *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1308 (Fed. Cir. 2007).

² To the extent SFI intends “and placing” to alter the scope of the claims, which require splitting, it is judicially estopped from doing so. *See infra*.

Further, when the specification “consistently” and “exclusively” describes an element in a certain manner in various embodiments, that is “clearly” what the inventor invented, and informs (and limits) the proper construction of such elements. *GPNE Corp. v. Apple Inc.*, 830 F.3d 1365, 1370–71 (Fed. Cir. 2016) (holding that district court did not err in characterizing a “node” as a “pager” where specification consistently and exclusively described invention as a system of pagers); *Wisconsin Alumni Rsch. Found. v. Apple Inc.*, 905 F.3d 1341, 1350–51 (Fed. Cir. 2018) (finding that a “prediction” was limited to a dynamic prediction due to exclusive use in the specification); *Eon Corp. IP Holdings v. Silver Spring Networks*, 815 F.3d 1314, 1320–23 (Fed. Cir. 2016) (holding that although terms “portable” and “mobile” might theoretically, in the abstract, be interpreted broadly as anything that is capable of being moved, specification’s extensive discussion and use of terms mandates constructions that are tethered to patent’s description of the invention); *Nystrom v. TREX Co.*, 424 F.3d 1136, 1144–45 (Fed. Cir. 2005) (construing “board” to mean “wood cut from a log” in light of specification’s consistent use of term, because patentee “is not entitled to a claim construction divorced from the context of the written description and prosecution history”). That is true here as well.

In its Complaint (before SFI saw Google’s source code and evidence of the accused products), SFI interpreted the term “generating” consistent with Google’s construction. SFI’s Complaint stated that its patents require “parsing and splitting the data into different portions before storage.” Compl. ¶ 15; *see also id.* at ¶¶ 22–23. SFI’s opposition to Google’s 101 brief similarly interpreted the patents as covering “splitting.” Dkt. 42 at 2 (“The ’854 and ’609 Patents are in the same family and claim specific implementations of SFI’s unique cryptographic splitting technology.”); *see also id.* at 1, 3, 28.

Even more, the Court relied on SFI’s interpretation of the claims in the Complaint by

stating that “the claims are directed to a method for securing data that involves splitting data, encrypting the data with encryption keys, and storing the data and the encryption keys in one or more places.” Dkt. 125 at 2; *see also id.* at 40-41 (the asserted patents “require[] parsing data into chunks, encrypting those chunks with different encryption keys, further encrypting the chunks with another key, and storing each chunk with data indicative of a key on a storage device”). Indeed, this interpretation is part of why the Court found in favor of SFI and denied Google’s Motion to Dismiss based on that interpretation. Dkt. 125 at 42 (“[t]he ‘purportedly innovative technological solution’ of these claims [being] rooted in *the particular sequence of parsing*, encrypting, and storing steps they describe”); *see also id.* at 48 (finding an inventive concept in “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”) (*quoting* Compl. ¶ 23). SFI is accordingly judicially estopped from eliminating, through claim construction, a limitation that proved critical to surviving Google’s motion.³ *Trustees of Columbia Univ. in City of New York v. NortonLifeLock, Inc.*, No. 3:13CV808, 2019 WL 7040931, at *4-6 (E.D. Va. Dec. 20, 2019).

II. DATA INDICATIVE OF ... KEY(S) ('140 CL. 1; '854 CL. 1; '609 CL. 1, 2, 3)

Google: “metadata about ... key(s); not an encryption key”	SFI: No construction necessary. In the alternative: “information that points out, points to, makes known, shows, directs to, hints at, or suggests [at least one of the distinct encryption keys/a distinct encryption key/at least one of the different encryption keys/the at least one session key]”
---	---

Several asserted claims require storing data *indicative of* an encryption key with a secured share or chunk. *See, e.g.*, '140 cl. 1 (“include with each of the plurality of shares data indicative of

³ While unclear given the lack of actual contentions of infringement from SFI, it seems that SFI may be arguing that the plurality of shares or chunks can be populated with solely something other than the original data set. But the patents exclusively and repeatedly explain that the data from the data set (or data from encrypting the data set, not solely data from some other related information) is split into chunks or shares, and detail several algorithms for doing so. 53:40-55:47.

the at least one session key used to secure the dataset”), ’854 cl. 1 (“storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys”), ’609 cl. 1 (“storing [] at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys”).

The parties dispute whether the phrase, which is not a term of art, should be interpreted consistent with the intrinsic evidence, as Google provides, or whether it should not be construed at all or construed to include a grab bag of phrases that SFI contends, incorrectly, can also be somehow interpreted as the *key itself*, which is how SFI alleges this limitation is met in the accused Google products in its contentions of infringement. *See, e.g.*, ’140 Chart (Ex. L) at 34 (“Google stores with the shares data indicative of the at least one session key at least *by virtue of storing DEKs [Data Encryption Keys] with the data shares.*”) (emphasis added).

A. GOOGLE’S CONSTRUCTION IS SUPPORTED BY THE INTRINSIC EVIDENCE AND PLAIN MEANING OF THE PHRASE AT ISSUE

While the phrase “data indicative of” does not appear in the shared specifications, the patents make clear that “indicat[ing]” information is metadata: “*a meta-data block* may⁴ also be pre-pended to *indicate* information such as file length, encryption mode, key size, share ID, L/M/N share values, encryption key ID, encryption IV, hash mode, original buffer size, share buffer size, pre-encryption key ID, pre-encryption IV, pre-signature ID, pre-signature IV, and a flag indicating whether the a key transform such as package or AoNT transform was used to process the key.” 85:18-32. The specification further gives an exemplary data structure containing “information for identifying a key,” specifically the “unique identifier for this key” and the “length of buffer holding the id,” both of which the specification refers to as metadata above. *Id.* at 90:35-36; Fig. 49, Panel

⁴ The use of the permissive “may” merely shows that the indicative information need not be (and is not) included in all embodiments.

B.⁵ These consistent and exclusive disclosures inform and limit the interpretation of the corresponding claim element. *E.g.*, *GPNE Corp.*, 830 F.3d at 1370–71.

The specification also does not recite or suggest any information other than metadata that may “indicate” a key.⁶ Google’s construction thus appropriately makes explicit to the fact finder that the “data indicative of . . . key” cannot be the key itself. “There is no *per se* rule against negative constructions, which in some cases can be enough to resolve the relevant dispute.” *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 811 (Fed. Cir. 2021) (cleaned up). Even in dictionary definitions, the meaning of “indicate” is information that points to *something else*. *American Dictionary* (“indicate: 1. To show the way to or the direction of; point out. 2. To serve as a sign, symptom, or token of; signify”); *Webster’s Int’l Dictionary* (“indicate: to point out or point to or toward with more or less exactness : show or make known with a fair degree of certainty”). For instance, a street address like 123 Main St. indicates a physical location. It does not indicate the address itself. Likewise, a runny nose may indicate a cold, but a runny nose does not indicate a runny nose. Even SFI’s proposed construction, which appears to combine multiple definitions from the Oxford English Dictionary, does not state that the “information” can “indicate” itself.

Notably, when the Applicants wanted to claim the key itself, they did so. ’116 cl. 1 (“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”), 9, 15, 21 (reciting similar language). Such embodiments would also be covered by earlier unasserted

⁵ Note that this data structure does not include the key itself.

⁶ Here too, SFI’s Complaint uses a less expansive interpretation of the claim language, stating that storing “data indicative of at least one of the distinct encryption keys” with the data chunks was unconventional because it “would have been regarded as creating an insecurity by co-locating encrypted data with information which *might facilitate* decrypting such data.” Compl. ¶ 25.

patents that similarly explicitly recite storing the keys themselves. See, e.g., U.S. Patent No. 10,108,807 (Ex. O), cl. 1 (“storing the key on a portable device, wherein the portable device is different from the one or more storage devices”), 8, 16, 23; U.S. Patent No. 9,992,170 (Ex. P), cl. 7 (“storing the different keys on a key management server”), 14, 21. Of note, the corresponding independent claims of the ’170 patent also require that “the first plurality of shares includes data indicative of a cryptographic key used to secure the first data.” ’170 cl. 1, 8, 15. This evidences that when the Applicants wanted to claim the key itself, they did so explicitly. And when they wanted to claim something else, such as data indicative of the key, they also did so explicitly.

In sum, interpreting “data indicative of a key” to simply be “a key” effectively writes “data indicative of” out of the claim and renders “data indicative of” meaningless in the claim. *Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017) (“It is highly disfavored to construe terms in a way that renders them void, meaningless, or superfluous.”); *Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006) (“claims are interpreted with an eye toward giving effect to all terms in the claim⁷”).

B. SFI’S CONSTRUCTION IS NOT SUPPORTED BY THE INTRINSIC EVIDENCE AND DOES NOT AID THE FACT FINDER

SFI asserts that “data indicative of [] key(s)” need not be construed, but alternatively proposes numerous meanings for data indicative of a key cobbled together from definitions of “indicative” and “indicate”: “information that [1] points out, [2] points to, [3] makes known, [4] shows, [5] directs to, [6] hints at, or [7] suggests” the key. SFI Evidence at 4 (quoting *indicative*,

⁷ That is because “allowing a patentee to argue that physical structures and characteristics specifically described in a claim are merely superfluous would render the scope of the patent ambiguous, leaving examiners and the public to guess about which claim language the drafter deems necessary to his claimed invention and which language is merely superfluous, nonlimiting elaboration.” *Id.*; see also *Nautilus*, 572 U.S. at 901.

Oxford Dictionary (adj. 2. “That indicates, points out, or directs; that hints or suggests”), *indicate*, *Oxford Dictionary* (v. 1. “To point out, point to, make known, show (more or less distinctly)”).

Initially, SFI’s proposed alternative construction is not consistent with the specification. For example, nothing in the specification supports a meaning that “data indicative of a key” could be something that “hints at” or “suggests” a key. Indeed, these terms do not provide an objective basis to even evaluate infringement by the factfinder or a party attempting to avoid the patent. *Nautilus*, 572 U.S. at 901. What is or is not something that “hints at” or “suggests” a key in the context of the patents? By proposing multiple dictionary definitions divorced from the specification, SFI has adopted the *Texas Digital* approach that *Phillips* overruled, which was “improperly relied upon to condone the adoption of a dictionary definition entirely divorced from the context of the written description.” *Phillips*, 415 F.3d at 1321.⁸ Google’s construction, which is grounded in the specification and provides a clear description of this term, should be adopted.

Nor do any of the various terms that SFI proposes provide that “data indicative of a key” can be the key itself as SFI asserts. A key does not “hint,” “suggest,” “point to” etc... a key. It is the key as a matter of common sense. Ultimately, SFI’s interpretation of its own construction makes “indicative of” meaningless. Thus, even if SFI’s alternative construction is adopted, it should be made clear that “data indicative of key” cannot be the key itself. *Bicon*, 441 F.3d at 950.

⁸ See also *id.* at 1321-22: “Dictionaries, by their nature, provide an expansive array of definitions. General dictionaries, in particular, strive to collect all uses of particular words, from the common to the obscure. By design, general dictionaries collect the definitions of a term as used not only in a particular art field, but in many different settings. In such circumstances, it is inevitable that the multiple dictionary definitions for a term will extend beyond the construction of the patent that is confirmed by the avowed understanding of the patentee, expressed by him, or on his behalf, when his application for the original patent was pending. Thus, the use of the dictionary may extend patent protection beyond what should properly be afforded by the inventor’s patent.” (citation and quotations omitted)

III. DATASET / DATA SET (ALL CLAIMS)

Google: “collection of related information made up of separate elements that can be treated as a unit in data handling”	SFI: “a collection of information for storage”
--	---

All asserted claims require securing and storing a “data set” or a “dataset.” From the beginning of this litigation, despite Google’s repeated efforts, SFI has refused to identify any actual data set stored by the accused systems. Instead, SFI merely points to *data* allegedly stored by Google’s accused systems. *See e.g.* Dkt. 132 at 2-4 (collecting citations). The parties dispute whether a dataset is related information treated as a unit, *e.g.* a file or a database table (Google) or simply any data (essentially reading out “set” from these terms) (SFI).

A. THE INTRINSIC EVIDENCE CONSISTENTLY REFERS TO A “DATA SET” AS A UNIT

As the applicants demonstrated by using the word “data set” instead of “data,” the patents consistently depict the information secured by the claimed invention as related data treated as a unit. *See, e.g.*, 53:3-5 (equating a data set to a file type or entries within a database), 62:45-67 (equating a data set to a database or a document), 63:13-15 (equating a data set to flat files, data fields, or tables), 87:48-49 (equating a data set to a file or group of files).

The claims likewise distinguish between a data set and the data within that set, in accordance with Google’s construction. *See, e.g.*, ’609 cl. 1 (“wherein each data chunk of the plurality of data chunks comprises less than an entirety *of data of the data set*”). Interpreting “data” and “data set” to mean the same thing would violate canons of claim term differentiation, but also essentially read out the term “set” from the claim. *Bicon*, 441 F.3d at 950. Indeed, the claims do not make any sense if a “data set” is simply any “data.” For instance, claim 1 of the ’140 patent relates to a virtual disk that is presented to a client and which can reconstitute a stored dataset upon a request from the client. This requires that the client have some means of identifying the requested dataset, *e.g.* by selecting the filename or database entries it previously stored. But if the dataset is

simply any “collection of information” as SFI urges, then there is no unit or relation (*e.g.*, filename) which can be displayed to the client or selected by the client. The notion of a “virtual disk” makes little sense if that disk merely stores and displays blobs of data rather than related collections of data such as files or database entries.

B. THE EXTRINSIC EVIDENCE FURTHER SUPPORTS GOOGLE’S CONSTRUCTION

Both parties identified the same extrinsic evidence definition for “data set”: “a collection of related information made up of separate elements that can be treated as a unit in data handling.” *Microsoft 5th Dictionary*; SFI Evidence at 7 (proposing same); *see also Microsoft 4th Dictionary* (same definition). This definition is consistent with the specification. As explained above, the specification consistently shows that the information secured by the claimed invention comprises related data treated as a unit. This definition is also consistent with those provided by other references. *See, e.g., American Dictionary* (“data set”: “a collection of related data records on a computer-readable medium, such as a disk”). As both parties appear to agree the *Microsoft Dictionary* definition provides an appropriate baseline for what one of ordinary skill in the art would understand a “data set” to be, and as it comports not only with the specification but other extrinsic evidence of this term of art, it should be adopted.

Even though SFI takes its construction from the same *Microsoft Dictionary*, it removes almost all of it, keeping only that it is a “collection of information” and adding, as the claims elsewhere already provide, that it would be “for storage.” But SFI conspicuously removes that the “collection” is of “related information” and that the collection is “made up of separate elements that can be treated as a unit in data handling.” There is no apparent basis for this truncated definition beyond, here too, eliminating the meaning of the term to make it be “data” generally consistent with SFI’s apparent contentions of infringement. Google’s construction should be adopted.

IV. DATA SET / THE DATA SET

Google: “A data set” and “the data set” are the same data set.	SFI: No construction necessary.
---	--

It is black letter law that “the definite article ‘the’ particularizes the subject which it precedes. It is a word of limitation as opposed to the indefinite or generalizing force of ‘a’ or ‘an’.” *Warner–Lambert Co. v. Apotex Corp.*, 316 F.3d 1348, 1356 (Fed. Cir. 2003) (internal quotation omitted). In a patent claim, use of “the” preceding a claim element is interpreted to refer to an earlier recitation of the same claim element. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1356–57 (Fed. Cir. 1999). Google’s proposed construction follows this black letter law specifically such that “the data set” or “the dataset” in the claims refer back to “a data set” or “a dataset,” respectively, as previously used in the claims. *Infernal Tech., LLC v. Activision Blizzard Inc.*, No. 2021-2349, 2023 WL 370602, at *2–3 (Fed. Cir. Jan. 24, 2023) (finding that recitations of “observer data” in the patent must refer to the same data set, and the patent not infringed because the patent holder pointed to inconsistent sets of data).

For its part, SFI proposes “no construction necessary.” On the parties’ meet and confer, Google attempted to understand why, given this black letter law, SFI would not simply agree with Google’s construction. SFI appeared to agree that the claims should be interpreted as Google proposed. However, it contended that the jury need not be told of that reading because it is “obvious.”⁹

But it certainly is not “obvious,” based on SFI’s reading of the claims in its infringement

⁹ In accordance with this Court’s Scheduling Order (Dkt. 54), Google also identified several other terms which required antecedent basis, and provided constructions listing those bases. Exs. Q, R. SFI refused to provide constructions for any of those other terms even though the Court’s Scheduling Order explicitly required that SFI provide constructions for all terms “collectively identified by the parties.” To the extent SFI is allowed to provide constructions for these other terms down the road, Google hopes that the Court’s resolution of this dispute now would eliminate dispute as to these other antecedent basis terms later in the case.

contentions, that it agrees with this clear reading of the claims, which is the reason that Google seeks to construe these terms here. Indeed, it appears SFI's position is a smoke screen. As discussed *supra*, SFI has repeatedly refused to identify the "data set" in its infringement contentions as required by the claims, and appears to contend that any "data" can be a data set and that the accused data set can be different for various iterations of the claimed "data set." For example, SFI has not even attempted to show that all instances of "data set" recited in the claims refer to the *same* "data set," again apparently contending that any data—including different data than before—can be "the data set." *See, e.g.*, '140 Chart (Ex. L) at 35-36 (failing to show or even allege that the reconstituted dataset is the same "dataset received from the client device"), 40-41 (appearing to allege the encrypted "dataset" is something other than the "dataset received from the client device"). Such allegations are improper. *Infernal Tech.*, 2023 WL 370602 at *2–3.

SFI should not be permitted to have wiggle room to argue a different meaning to the jury for these terms where even it appears to agree—as it must—that Google's proposal is correct from the plain language. Google's construction should be adopted. *O2 Micro*, 521 F.3d at 1361 (a "dispute over the scope of the asserted claims is a question of law" and "must be resolved by the court").¹⁰

V. VIRTUAL DISK [I] COMPRISING A DIRECTORY MAPPED TO THE PLURALITY OF PHYSICAL STORAGE DEVICES ('140 CL. 1)

Google: "a distributed file system shared among file servers that includes a directory with a clients' view of all file assets mapped to the physical storage devices on which they are stored"	SFI: No construction necessary. In the alternative: "a system that simulates or emulates a physical storage device, comprising a directory mapped to a plurality of physical storage devices such that physical locations of the shares are hidden from the client device"
--	--

¹⁰ SFI cited, as "extrinsic evidence" with its preliminary constructions, *SFA Sys., LLC v. 1-800-Flowers.com, Inc.*, 940 F. Supp. 2d 433, 447 (E.D. Tex. 2013); *Cybergym Rsch. LLC v. Icon Health & Fitness, Inc.*, 2007 WL 5688735, at *22 (E.D. Tex. Jan. 25, 2007), where the Court declined to adopt a construction regarding antecedent basis because the language was clear. But here, SFI's positions and disclosures to date show a material dispute that must be resolved.

Claim 1 of the '140 patent recites “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.” At the time of the '140 Patent, “Virtual disk” was a term of art that referred to a RAM implementation of a traditional disk drive. *Microsoft 4th Dictionary* (“virtual disk: *See* RAM disk”) (“RAM disk: Short for random access memory disk. A simulated disk drive whose data is actually stored in RAM memory.”); *Newton's Dictionary* (“Virtual Disk: A portion of RAM (Random Access Memory) assigned to simulate a disk drive. Also called a ram disk.”). SFI does not meaningfully dispute this. Indeed, it does not provide any actual extrinsic evidence for this term.¹¹

There is no dispute, however, that the '140 patent does not use this known meaning in the art, as neither the claims nor the specification make any reference to implementing a disk drive in RAM or make any suggestion that is how the term is used in the '140 patent. Nor does the term “virtual disk” appear anywhere in the specification. However, the concept recited in '140 claim 1 does appear at Col. 87, lines 16-24:

A Parsed File System (PFS) is a distributed file system which incorporates a directory, shared among file servers, which is itself parsed. The PFS directory is the clients' view of all file assets. The set of files visible to an individual client is controlled by that client's group keys. The PFS may maintain a directory that contains information about the locations of the shares (for example, the file server location) and the names of the files at the share locations that include the share data.

Since the claim requires not only a “virtual disk” but a “virtual disk [] comprising a directory mapped to the plurality of physical storage devices,” Google's construction includes the specification's explanation as to how that is accomplished: by “includ[ing] a directory with a clients' view of all file assets mapped to the physical storage devices on which they are stored.”

¹¹ SFI oddly labels the *case law* it cites, discussed below, as “extrinsic evidence.” It is unclear how case law is extrinsic evidence, but to the extent SFI intended to refer to the patent in that case as extrinsic evidence, it is addressed below also.

Nystrom, 424 F.3d at 1144 (construing “board” as “wood cut from a log” based on the specification’s consistent use).

SFI asserts that the “virtual disk” phrase does not require construction. This might be true if the patent used “virtual disk” in a manner consistent with the plain and ordinary meaning of this term in the art, and if the jury somehow knew that technical meaning. However, that is a moot point as it is clear that SFI is not reading the term that way and the ‘140 patent does not use it that way. Rather, SFI’s alternative proposal merely replaces “virtual disk” with “a system that simulates or emulates a physical storage device.” This is neither the ordinary technical meaning (RAM disk), nor does it track the “Parsed File System” that performs the recited function in the specification.

SFI cites *Oasis Rsch., LLC v. AT&T Corp.*, 2012 WL 602199, at *9 (E.D. Tex. Feb. 23, 2012), as supposedly supporting its construction. There, the patent at issue acted as its own lexicographer for the terms “virtual device” and “virtual disk drive”: “***In the context of this patent specification***, a ‘virtual device’ is an arrangement that ‘simulates’ or ‘emulates’ a locally-attached, physical device. For example, a ‘virtual disk drive’ can be an arrangement (e.g., some combination of local and/or remote hardware and/or software) that ‘looks like’ a physical disk drive.” *Id.* at *6-7. The court essentially adopted this construction, noting that “[i]n the specification, a patentee may define his own terms and act as his own lexicographer. *Phillips*, 415 F.3d at 1316.”¹² *Id.* at *8. Plainly, a lexicographical construction based on an unrelated patent’s specification is not applicable here and certainly does not establish an “ordinary meaning” known to those in the art contrary to contemporaneous technical dictionaries or otherwise. And as with “data set,” SFI

¹² *Phillips* states that “our cases recognize that the specification may reveal a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess. In such cases, the inventor’s lexicography governs.” 415 F.3d at 1316.

appears to have taken a dictionary definition and removed portions that are inconsistent with its infringement theories: here, that that physical device is emulated in RAM. SFI's proposal is thus untethered from the evidence and should be rejected.

VI. EXTERNAL KEY ('854 CL. 1)

Google: “a key generated by a third party” OR Indefinite	SFI: No construction necessary. In the alternative: “a key stored separately from the data chunks”
--	--

Claim 1 of the '854 patent requires “receiving an external key from an external storage system.” The parties dispute whether an “external key” is generated by an external entity, which in the context of the patents is a third party (Google's construction), or merely stored “separately” from the data chunks and not necessarily “external” at all (SFI's construction). This dispute is important because SFI seeks to read the '854 patent to cover keys and systems *internal* at Google and thus not “external” at all.¹³

Claim 1 of the '854 patent ultimately uses the external key to further secure the encrypted data chunks by “performing an encryption operation based on the external key to further secure the plurality of data chunks.” Consistent with Claim 1, the specification repeatedly discusses using keys or other information from sources external to the encryption system, i.e., from third parties, to further secure data. For example, the patent explains that “the enrollment process may issue multiple digital certificates from multiple certificate authorities, including one or more proprietary certificate authorities internal or external to the trust engine” (24:27-34) and that “the certificate authority 115 may advantageously comprise a trusted *third-party organization or company* that

¹³ For example, while the allegations are not clear, it appears that for the external key (and external storage system) SFI is pointing to keys in Google's *internal* Keystore system. '854 Chart (Ex. M) at 2 (“Google's encryption technology receives an external 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.'”).

issues digital certificates, such as, for example, VeriSign, Baltimore, Entrust, or the like.” 11:48-51 (emphasis added). Alternately, “the data vault may be implemented by a *third-party system*” that “serve[s] the requested sensitive data *after the third-party system receives a signal* indicating positive user authentication from the trust engine.” 29:49-54. The patents may also encrypt data using a third party’s public key, so that only that third party can decrypt the data. 32:30-59. The patents may also use external keys from an external key management service, in the event a user or client wants to manage their own keys. 56:4-18, 57:66-58:32. This is consistent with the remainder of the disclosures of key management in the specification, which repeatedly show that the keys can be managed by the user of the system or some other system external to that user/system. 56:4-18, 81:58-61; ’854 patent at 77:59-78:8, 78:66-79:23. This allows a data owner who does not completely trust the data storer to maintain control of the keys used to decrypt that stored data.

SFI contends that “external key” need not be construed. At the parties’ meet and confer, Google asked SFI how the jury could discern whether a key was “external” without a construction. SFI said that a jury would simply look at an accused key and decide whether it is external or not. This dodges the question of what the key is “external” *to*: the data, a server, a system, or an entity. But even more, SFI improperly assigns the role of determining the metes and bounds of the claim to the jury. *O2 Micro*, 521 F.3d at 1360 (“When the parties raise an actual dispute regarding the proper scope of these claims, the court, not the jury, must resolve that dispute.”).

Indeed, it is apparent from SFI’s alternative construction that it is interpreting “external” to mean something *other* than even the plain and ordinary meaning of “external” or even how it is used in the specification (i.e., third party). Rather, SFI contends that to be “external” a key need only be “separate.” “Separate” is not even the plain language meaning of “external.” SFI’s own

cited extrinsic evidence shows this, defining “external” as “[s]ituated or lying outside; pertaining to, or connected with, the outside or outer portion of anything.” *Oxford Dictionary* at 1. So does common sense. An external window is generally not “separate” from a building, and a “separate” bathroom can be internal to or external from a house.

SFI’s “stored separate from a key” language is similarly nonsensical in the context of the intrinsic evidence. Claim 1 of the ’854 patent requires “receiving an external key *from* an external storage system.” Thus, it is “external” when it is received based on where it comes from, i.e., a third party, as the intrinsic evidence makes clear as shown above. Indeed, the claim says nothing about “storing” the external key at all after it’s received. To the extent that SFI’s construction is intended to refer to separate storage before the external key is received, then it is unclear for all the reasons discussed above as to what it means to be separate—a separate computer, a separate location in memory on the computer, a separate physical location? Here too, SFI’s invitation that the Court adopt an ambiguous and likely indefinite construction not grounded in the intrinsic evidence should be rejected. *Phillips*, 415 F.3d at 1327 (“[W]e have looked to whether it is reasonable to infer that the PTO would not have issued an invalid patent, and that the ambiguity in the claim language should therefore be resolved in a manner that would preserve the patent’s validity.”).

VII. MINIMUM NUMBER OF THE PLURALITY OF [DATA] CHUNKS (’854 CL. 1; ’609 CL. 1)

Google: “a predefined number of the lowest amount of the plurality of data chunks”	SFI: No construction necessary. In the alternative: “a threshold number of chunks less than or equal to the total number of [data] chunks”
---	--

Two asserted claims require that a data set split into data chunks must be able to be “reconstructed using at least a minimum number of the plurality of [data] chunks.” ’854 cl. 1; ’609 cl. 1. The parties dispute whether there must be some actual “minimum” number (Google) or

whether this limitation simply refers to whatever number of chunks is ultimately used to reconstitute the data set, rendering the phrase essentially meaningless (SFI).

The Summary of the Invention notes that the “data splitting process” may “prohibit[] reconstruction without a predetermined portion [of shares] from more than one location in one depository or from multiple depositories.” 3:20-30; *see also C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 864 (Fed. Cir. 2004) (finding that statements made in the “summary of the invention” section of a patent are “more likely to contain statements that support a limiting definition of a claim term than other sections” because they are more likely to “describe the invention as a whole”). The specification further explains this process in more detail: “[a]ccording to the present invention, fewer than all portions of the separated data generated by the secure data parser may be necessary in order to retrieve the original data. That is, out of m portions stored, n may be the minimum number of these m portions necessary to retrieve the original data, where $n \leq m$.” 69:9-23. For example, the system may be configured such that only two out of four portions are needed to recover the original data set. 69:9-23, 73:23-36. Or the system may be configured such that four out of four portions need to be used. 76:62-77:4.

In all these examples both the number of total shares and the number of required shares is known and configured, i.e., “predetermined,” in the security system itself.¹⁴ 81:18-34. “When a patent thus describes the features of the ‘present invention’ as a whole, this description limits the scope of the invention.” *Verizon*, 503 F.3d at 1308. And when the specification “consistently” and “exclusively” describes an element in a certain manner in various embodiments, that is “clearly”

¹⁴ This is possible because the claimed system can fix the number of shares. *See, e.g.*, ‘854 patent at 78:11-62 (“In some embodiments, the data may be split into a predefined number of shares”); Figs. 21-24. Thus if the claimed system has been configured to split datasets into four shares, it will create 1 MB shares upon receiving a 4 MB dataset, 100 MB shares upon receiving a 400 MB dataset, etc.

what the inventor invented, and informs (and limits) the proper construction of such elements. *GPNE Corp.*, 830 F.3d at 1370–71; *Wisconsin Alumni*, 905 F.3d at 1350–51; *Eon Corp.*, 815 F.3d at 1320–23; *Nystrom*, 424 F.3d at 1144–45.

Further, not all asserted claims include the “minimum number” language. For example, claims 1 and 9 of the ’116 patent require “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.” And claim 1 of the ’140 requires “generat[ing] 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.” That the ’854 and ’609 claims have additional “minimum number” verbiage suggests that language is intended to further limit the scope of those claims. *Wasica Fin.*, 853 F.3d at 1288 n.10.

SFI asserts that the “minimum number” limitation need not be construed, again presumably suggesting the jury will simply “know” what that phrase means. However, SFI’s alternate proposal shows that SFI interprets the phrase to have no meaning at all. In fact, at the meet and confer on claim construction, SFI stated that whatever number of shares are ultimately used to reconstruct the data set would meet the “minimum number” limitation. So according to SFI, whether 4, 40, 400, or 40,000 chunks are ultimately required to reconstruct the data set, that would be “a threshold number of chunks less than or equal to the total number of [data] chunks” because each would be the amount actually used to reconstruct the data set. SFI’s infringement contentions reflect this vacuous interpretation, as they do not show how the “minimum number” limitation is met and barely mention it at all. *See, e.g.*, Compl. ¶ 73; ’854 Chart (Ex. M) at 4. SFI’s efforts to read out this claim limitation and make it meaningless should be rejected. *Bicon*, 441 F.3d at 950. Google’s construction should be adopted.

VIII. SEPARATELY STORING EACH DATA CHUNK OF THE PLURALITY OF DATA CHUNKS TOGETHER WITH ONE OF THE PLURALITY OF OBFUSCATED DIFFERENT ENCRYPTION KEYS ('116 CL. 1)

Google: “separately storing each data chunk of the plurality of data chunks with a key other than the key that encrypts that chunk on a plurality of different storage devices”

SFI: No construction necessary.
In the alternative: “separately storing each data chunk of the plurality of data chunks together with one of the plurality of different encryption keys that has been rendered unclear or obscure”

Claim 1 of the '116 patent requires “separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys.” The parties dispute what this phrase requires to obfuscate a key. Specifically, the dispute is whether the obfuscating is accomplished by storing keys with chunks other than the chunk it encrypted as exclusively taught by the patents (Google), or whether it need be construed at all, or given a construction that has no grounding in, and makes no sense with, the use of the phrase in the intrinsic evidence (SFI).

A. THE INTRINSIC EVIDENCE SUPPORTS GOOGLE’S PROPOSAL

The text of the specification refers to obfuscating once, in stating that “[t]he original data processed as described in this embodiment is encrypted *and* obfuscated and is secured.” 53:31-32.

The Figures similarly show that obfuscating is a different operation than encryption:

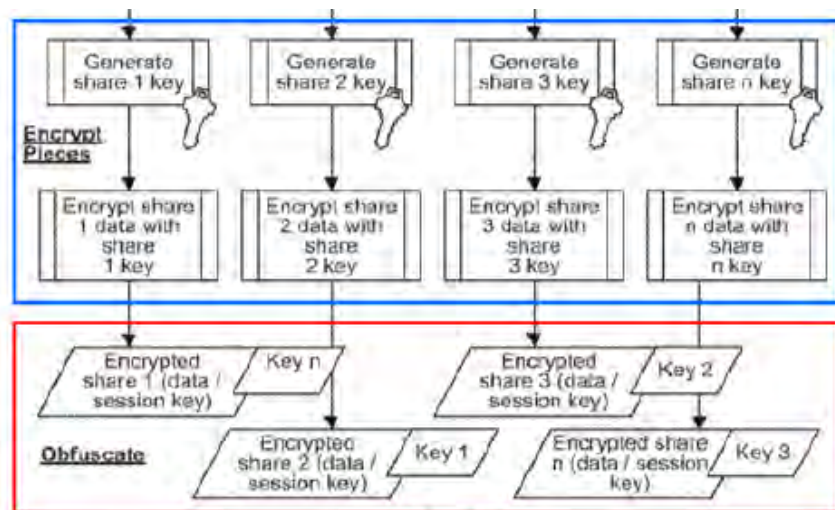


FIG. 21

Fig. 21 (excerpted and annotated); *see also* Figs. 22-24. As the figures demonstrate, during the encryption phase (in blue), share 1 is encrypted with key 1, share 2 is encrypted with key 2, etc. And during the obfuscate phase (in red), share 1 is stored with key n, share 2 is stored with key 1, etc. Obfuscating is plainly a different step than encrypting. And it involves storing each key with a different share than the share it encrypted, just as in Google’s construction.

This is the specification’s only explanation of what “obfuscate” could possibly mean in the context of the technology at issue in the patents.¹⁵ Again, when the specification “consistently” and “exclusively” describes an element in a certain manner in various embodiments, that is “clearly” what the inventor invented, and informs (and limits) the proper construction of such elements. *E.g.*, *GPNE Corp.*, 830 F.3d at 370–71.

B. SFI’S PROPOSAL IS UNTETHERED FROM THE TEACHINGS OF THE PATENTS

SFI’s “plain meaning” construction of “render[] unclear or obscure” is not grounded in the specification, and it is difficult to understand how it would even be applied objectively by one skilled in the art, much less a jury. Both parties cited extrinsic evidence which states that “obfuscating” information makes it difficult—but not impossible—to understand. *American Dictionary* (“obfuscate: To make so confused or opaque as to be difficult to perceive or understand.”); *Webster’s Int’l Dictionary* (“obfuscate: “to make difficult of comprehension or interpretation . . . [;] to make unnecessarily complex usu. to the point of confusion”); *Oxford Dictionary* (“obfuscate: to darken, obscure (the understanding, judgment, etc.)”).

While this meaning of obfuscate may make sense in terms of telling a houseguest you have obscured a physical key to your home under a rock, SFI provides no basis as to how it could be

¹⁵ At the meet and confer, SFI was unable to recite any other teachings in the specification regarding how to obfuscate data.

applied sensibly and objectively in claim 1 of the '116 patent. At what point would a key be sufficiently “obscured” or “unclear” so as to be obfuscated? When would it be sufficiently “difficult” to understand? Indeed, such efforts would likely render the claim indefinite, as a person of skill in the art would not have objective boundaries to determine whether a given action had sufficiently rendered the data “unclear or obscure.” This is shown by the very definition of “obscure” that SFI cites: “Not manifest to the mind or understanding; imperfectly known or understood; not clear or plain; hidden, doubtful, vague, uncertain.” SFI Evidence at 4 (quoting from *Oxford Dictionary*). *Nautilus*, 572 U.S. at 901 (“a patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention”); *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1372–74 (Fed. Cir. 2014) (finding the phrase “unobtrusive manner that does not distract a user” indefinite for failing to provide objective boundaries). As SFI’s construction requiring such a subjective analysis would render the claim indefinite, it should be rejected.¹⁶ *Phillips*, 415 F.3d at 1327.

IX. TRANSFORMING / PERFORMING A TRANSFORM ('116 CL. 2, 9)

Google: “changing without the use of a secret key the bits of a key / data indicative of a key”	SFI: No construction necessary. In the alternative: “changing the form”
--	---

Claim 9 of the '116 patent recites “transforming each of the plurality of different encryption keys.” Claim 2 depends from the “obfuscating” claim 1 discussed *supra* and further requires

¹⁶ SFI additionally cites as “extrinsic evidence” an IBM branded presentation with no date, no author, no suggestion as to the specific purpose of the document, and that is marked “Attorney’s Eyes Only.” SFI Evidence at 5, citing ORSINI_000005021 at -5026 (Ex. S). This secret extrinsic evidence does not move the needle against the intrinsic evidence. *Honeywell Int’l, Inc. v. Int’l Trade Comm’n*, 341 F.3d 1332, 1341 (Fed. Cir. 2003) (rejecting a construction that was only supported by confidential documents, as it would “import a limitation that is not only outside the bounds of the claims, the written description, and the prosecution history, but is also outside the scope of any written publication”).

“obfuscating each of the plurality of different encryption keys comprises *performing a transform* on data indicative of at least one of the plurality of different encryption keys.” The parties dispute whether this “transform” should be interpreted to perform the only type of “transform” disclosed in the ’116 patent (Google) or whether it should not be construed at all or construed to require any type of change at all, which is not even consistent with the lay dictionary meaning of “transform” (SFI). As with the obfuscating phrase in the prior section, SFI seeks this expansive definition not grounded in the intrinsic or extrinsic evidence to accuse encryption in the accused Google products. ’116 Chart (Ex. N) at 12 (“***Google transforms*** each of the different encryption keys ***when it encrypts*** the DEKs using the KEKs.”) (emphasis added). SFI thus seeks to interpret both “obfuscating” and “transforming” to cover encrypting, notwithstanding that the claims explicitly state when they call for “encrypting.”

“Transform” has a meaning in the art. Specifically, the specifications explain that “an All or Nothing Transform (AoNT), such as a Full Package Transform, may be used to further secure data by transforming splitting keys, encryption keys, any other suitable data elements, or any combination thereof.” 75:34-56; *see also* 81:15-17 (“The key may then be transformed for splitting and storage such as with a package transform or AoNT as described herein.”) All or Nothing Transforms were introduced in Ronald L. Rivest’s 1997 paper “All-Or-Nothing Encryption and The Package Transform.” (Ex. T). That paper, which is cited by the asserted patents, explains that all or nothing transformations change the bits of a message such that “[i]t is computationally infeasible to compute any function of any message block if any one of the pseudo-message [transformed message] blocks is unknown”—hence the “all or nothing” moniker. *Id.* at § 3. It further explains that “an all or nothing transformation is not itself ‘encryption,’ since it makes no use of any secret key information” (*id.*), in accordance with Google’s construction. The

specifications do not provide any further examples of how to “transform” an encryption key. Google’s proposal accords with this teaching and should be adopted. *E.g.*, *GPNE Corp.*, 830 F.3d at 370–71.

For its part, SFI asserts what it presumably believes should be the “plain and ordinary” (not term of art) meaning of transforming. But even were such a construction appropriate here, SFI’s “changing the form” construction does not even comport with that plain meaning. “Transforming” in lay terms ordinarily refers to a *significant or substantial* change, not just any change. *American Dictionary* (“transform: 1. To change markedly the appearance or form of. 2. To change the nature, function, or condition of; convert.”); *Webster’s Int’l Dictionary* (“transform: to change completely or essentially in composition or structure”). Even SFI’s proffered extrinsic evidence requires changes that are substantial enough to alter the appearance or format of data. SFI Evidence at 6 (*quoting Microsoft 5th Dictionary*: “transform: To change the appearance or format of data without altering its content; that is, to encode information according to predefined rules”).

Yet under SFI’s construction, any changes to the “form,” whatever that means in the context of an encryption key, would be considered transformations. The ambiguity becomes even more clear when looking to apply SFI’s construction in the claims, which require “transforming . . . different encryption keys” that were used to “encrypt[] each of the data chunks.” The patents explain that a key is “a generated random number” (53:19-21), e.g., a key could be 4,643,726,097. It is unclear how one would “change the form” of 4,643,726,097. Replace the commas with periods or spaces, as is common in other parts of the world? Express it in scientific notation, as 4.643×10^9 ? Here again, SFI’s interpretation of the claim would render it indefinite. *Nautilus*, 572 U.S. at 901; *Interval Licensing*, 766 F.3d at 1372–74. As noted above, the specification *is* clear that “an

All or Nothing Transform (AoNT), such as a Full Package Transform,” is used consistent with Google’s construction. SFI’s construction should be rejected and Google’s adopted.

X. SESSION KEY (’140 CL. 1, 8)¹⁷

Google: “key generated each time a data set is secured”	SFI: “a key created to both secure and restore a specific collection of information”
--	---

As SFI’s extrinsic evidence states, a “session” in the context of computer technology ordinarily refers to the period of time during which a program or communication connection is running.¹⁸ Google’s construction tracks this plain meaning of “session” as well as the use of the “session key” in the specification as a key that is generated when a data set is secured. 32:36-52; 56:19-41, 56:53-57:13, 57:25-54, 57:66-58:33. SFI proposes that a “session key” be a “key created to both secure [*i.e.* encrypt] and restore [*i.e.* decrypt]” information. But that is how the specification defines a “symmetric” key. 32:40-43. While the specification does state that in a preferred embodiment symmetric keys may be used (32:36-47), it elsewhere notes a “skilled artisan will recognize from the disclosure herein that the cryptographic keys may advantageously include some or all of symmetric keys, public keys, and private keys.” 11:40-45.

¹⁷ Only SFI identified this term for construction. At the parties’ meet and confer, Google asked what dispute or issue in the case the meaning of this term related to. SFI said only that the jury would likely not know what the term means. This is inconsistent with its position for almost every other term before the Court. Thus, it is possible there is a latent dispute with this term that SFI has not actually disclosed.

¹⁸ *Microsoft 5th Dictionary* (“session: 1. The time during which a program is running. . . . 2. In communications, the time during which two computers maintain a connection.”); Charles C. Mann, *A Primer on Public-key Encryption*, THE ATLANTIC, p. 6 (Sept. 2002 issue) (Ex. U) (referring to a “session key” as a key one would “only use for a short time” for a single round of messages); *see also Newton’s Dictionary* (“session: 1. An active communications connection, measured from beginning to end, between computers or applications over a network. . . .”).

Dated: December 6, 2023

Respectfully submitted,

/s/ Stephen E. Noona
Stephen E. Noona (VSB No. 25367)
KAUFMAN & CANOLES, P.C.
150 W. Main Street, Suite 2100
Norfolk, VA 23510-1665
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

David A. Nelson (*pro hac vice*)
Nicholas D. Caspers (*pro hac vice*)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401
davenelson@quinnemanuel.com
nicholascaspers@quinnemanuel.com

David Perlson (*pro hac vice*)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700
davidperlson@quinnemanuel.com

Deepa Acharya (*pro hac vice*)
Kevin Hardy (*pro hac vice*)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
1300 E Street NW, Suite 900
Washington, DC 20001
Telephone: (202) 538-8107
Facsimile: (202) 538-8100
deepaacharya@quinnemanuel.com
kevinhardy@quinnemanuel.com

Dawn M. David (*pro hac vice*)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
2755 E. Cottonwood Pkwy., Suite 430

Salt Lake City, UT 84121
Telephone: (801) 515-7300
Facsimile: (801) 515-7400
dawndavid@quinnemanuel.com

Counsel for Google LLC