

Filed on behalf of Google LLC by:

Paper No. ____

Elisabeth H. Hunt, Reg. No. 67,336
Gregory S. Nieberg, Reg. No. 57,063
Nathan R. Speed (admitted *pro hac vice*)
WOLF, GREENFIELD & SACKS, P.C.
600 Atlantic Avenue
Boston, MA 02210
(617) 646-8000 Phone
(617) 646-8646 Fax

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC
Patent Owner.

Case No. IPR2024-00215
Patent No. 10,452,854

PETITIONER'S REPLY TO PATENT OWNER RESPONSE

TABLE OF CONTENTS

I.	Ground 2: Claims 1-10 Are Unpatentable over Foster-Hayhurst	1
A.	Hayhurst is Analogous Art.....	2
1.	Hayhurst is in the patent’s field of endeavor.....	2
2.	Hayhurst is reasonably pertinent to problems the ’854 patent relates to.....	5
B.	POSAs Had Motivation For Foster-Hayhurst.....	6
1.	Foster stores encrypted content.	7
2.	Foster-Hayhurst is consistent with Foster’s goals.	10
C.	Foster-Hayhurst Has <i>Data Chunks</i>	13
II.	Ground 1: Claims 1-10 Are Unpatentable over Orsini.....	16
A.	POSAs Would Have Encrypted Orsini’s Share Keys Using a Conventional KEK.....	17
1.	The Board Misunderstood the Petition’s Obviousness Argument.	20
2.	Petitioner Does Not Rely on Common Sense To Supply a Missing Limitation.....	21
3.	SFI’s Challenges to Petitioner’s Motivation-to-Combine Theory Fail.....	22
a.	POSAs Would Have Wanted to Increase Orsini’s Security.	23
b.	The Alleged Drawbacks to KEKs Were Easily Overcome and Are Legally Irrelevant.	25
c.	Petitioner’s Motivation-to-Combine Theory Is Not Based on Hindsight, It Is Grounded in Evidence.	27
B.	SFI’s Reasonable Expectation of Success Challenge Fails	28

TABLE OF AUTHORITIES

Cases

<i>Arendi S.A.R.L. v. Apple, Inc.</i> , 832 F.3d 1355 (Fed. Cir. 2016)	22
<i>Axonics, Inc. v. Medtronic, Inc.</i> , 75 F.4th 1374 (Fed. Cir. 2023)	14
<i>Cole Kepro Int’l, LLC v. VSR Indus., Inc.</i> , 2017 WL 2627982 (Fed. Cir. 2017)	25
<i>Corephotonics, Ltd. v. Apple Inc.</i> , No. 2020-1961, 2021 WL 4944471 (Fed. Cir. Oct. 25, 2021)	13, 27
<i>CyWee Grp. Ltd. v. ZTE (USA), Inc.</i> , 90 F.4th 1358 (Fed. Cir. 2024)	27
<i>DSS Tech. Mgm’t v. Apple Inc.</i> , 85 F.3d 1367 (Fed. Cir. 2018)	22
<i>Fleming v. Cirrus Design Corp.</i> , 28 F.4th 1214 (Fed. Cir. 2022)	22
<i>Google LLC v. Nobots LLC</i> , IPR2022-00940, Paper 38 (Nov. 23, 2023)	28
<i>In re Asset Guard Prods., Inc.</i> , 2022 WL 1097363 (Fed. Cir. Apr. 13, 2022)	5
<i>In re Clay</i> , 966 F.2d 656 (Fed. Cir. 1992)	4
<i>In re Cree, Inc.</i> , 818 F.3d 694 (Fed. Cir. 2016)	27
<i>In re Mouttet</i> , 686 F.3d 1322 (Fed. Cir. 2012)	7
<i>In re Wood</i> , 599 F.2d 1032 (C.C.P.A. 1979)	2

<i>Intel Corp. v. PACT XPP Schweiz AG</i> , 61 F.4th 1373 (Fed. Cir. 2023)	19-20, 26
<i>Koninklijke Philips N.V. v. Google LLC</i> , 948 F.3d 1330 (Fed. Cir. 2020)	22
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	4
<i>Netflix, Inc. v. DivX, LLC</i> , 80 F.4th 1352 (Fed. Cir. 2023)	4
<i>Randall Mfg. v. Rea</i> , 733 F.3d 1355 (Fed. Cir. 2012)	21
<i>Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.</i> , 66 F.4th 1373 (Fed. Cir. 2023)	2
<i>Teva Pharm. Indus. Ltd. v. AstraZeneca Pharms. LP</i> , 661 F.3d 1378 (Fed. Cir. 2011)	16
<i>Voda v. Cordis Corp.</i> , 536 F.3d 1311 (Fed. Cir. 2008)	15
<i>Wang Labs., Inc. v. Toshiba Corp.</i> , 993 F.2d 858 (Fed. Cir. 1993)	4
<i>Wyers v. Master Lock Co.</i> , 616 F.3d 1231 (Fed. Cir. 2010)	4

APPENDIX LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 10,452,854 (“’854 patent”)
1002	Prosecution History of U.S. Patent No. 10,452,854
1003	Declaration of Samrat Bhattacharjee, Ph.D. (“Bhattacharjee”)
1004	Curriculum Vitae of Samrat Bhattacharjee, Ph.D.
1005	U.S. Patent Application Publication 2004/0049687A1 (“Orsini”)
1006	U.S. Patent Application Publication 2003/0200176A1 (“Foster”)
1007	U.S. Patent Application Publication 2004/0216164A1 (“Hayhurst”)
1008	RESERVED
1009	Security First Innovation’s 2023-08-14 Infringement Contentions, Chart A in <i>Security First Innovations, LLC v. Google LLC</i> , 2-23-cv-00097 (E.D. Va.)
1010	Redline Comparison of U.S. Patent Application Publication 2004/0049687A1 to U.S. Patent No. 10,452,854
1011	U.S. Patent No. 5,991,414
1012	U.S. Patent Application Publication No. 2002/0169842
1013	U.S. Patent No. 6,393,568
1014	U.S. Patent No. 6,868,160
1015	U.S. Patent Application Publication No. 2006/0053112
1016	U.S. Patent Application Publication No. 2004/0005061
1017	U.S. Patent No. 5,412,722
1018	U.S. Patent No. 7,689,829
1019	U.S. Patent Application Publication No. 2003/0081784
1020	U.S. Patent No. 7,634,650
1021	U.S. Patent Application Publication No. 2004/0143733
1022	U.S. Patent Application Publication No. 2002/0126850
1023	U.S. Patent No. 5,812,671
1024	U.S. Patent Application Publication No. 2003/0012386

Exhibit	Description
1025	U.S. Patent No. 5,963,646
1026	U.S. Patent No. 5,416,841
1027	U.S. Patent No. 7,251,828
1028	U.S. Patent Application Publication No. 2003/0167314
1029	U.S. Patent No. 6,598,161
1030	U.S. Patent Application Publication No. 2005/0198490
1031	U.S. Patent Application Publication No. 2002/0169808
1032	U.S. Patent No. 6,345,101
1033	U.S. Patent No. 8,707,034
1034	U.S. Patent Application Publication No. 2003/0105719
1035	U.S. Patent No. 4,238,853
1036	U.S. Patent No. 6,819,766
1037	U.S. Patent Application Publication No. 2004/0172476
1038	U.S. Patent Application Publication No. 2004/0177257
1039	U.S. Patent No. 7,885,405
1040	U.S. Patent Application Publication No. 2005/0210269
1041	U.S. Patent Application Publication No. 2005/0120065
1042	RESERVED
1043	U.S. Patent Application Publication No. 2001/0037474
1044	U.S. Patent Application Publication No. 2003/0191938
1045	U.S. Patent Application Publication No. 2003/0028493
1046	U.S. Patent Application Publication No. 2003/0016820
1047	U.S. Patent Application Publication No. 2002/0042859
1048	U.S. Patent Application Publication No. 2003/0188153
1049	International Application Publication No. WO 2004/057461
1050	U.S. Patent No. 7,529,834
1051	U.S. Patent Application Publication No. 2006/0034457

Exhibit	Description
1052	U.S. Patent Application Publication No. 2005/0256972
1053	U.S. Patent Application Publication No. 2004/0049700
1054	U.S. Patent No. 5,675,653
1055	U.S. Patent Application Publication No. 2006/0062384
1056	U.S. Patent No. 6,490,353
1057	RESERVED
1058	RESERVED
1059	RESERVED
1060	RESERVED
1061	U.S. Patent Application Publication No. 2006/0059347
1062	U.S. Patent Application Publication No. 2006/0064386
1063	Rule 16(b) Scheduling Order in <i>Security First Innovations, LLC v. Google, LLC</i> , 2:23-cv-00097-JWK-RJK, Dkt. 54 (July 20, 2023)
1064	Google LLC's Proposed Claim Terms for Construction in <i>Security First Innovations, LLC v. Google, LLC</i> , 2:23-cv-00097-JWK-RJK (Nov. 11, 2023)
1065	Letter from A. Mayron to D. Perlson re Preliminary Proposed Constructions in <i>Security First Innovations, LLC v. Google, LLC</i> , 2:23-cv-00097-JWK-RJK (Nov. 11, 2023)
1066	U.S. Patent Application Publication No. 2004/0228479
1067	U.S. Patent Application Publication No. 2004/0039925
1068	Declaration of Nathan Speed ISO PHV Motion
1069	Telephone Hearing, Google v. SFI, IPR2024-00214, IPR2024-00215 (Mar. 21, 2024)
1070	Supplemental Declaration of Samrat Bhattacharjee, PH.D.
1071	Security First Innovations, LLC's Responses and Objections to Google LLC's First Set of Interrogatories (REDACTED by SFI) with Attached Charts A-D (Aug. 14, 2023) in <i>Security First Innovations, LLC v. Google LLC</i> , 2-23-cv-00097 (E.D. Va.) [SUPPLEMENTAL EVIDENCE – NOT FILED]

Exhibit	Description
1072	U.S. Patent Application Publication No. 2004/0019900
1073	U.S. Patent Application Publication No. 2002/0083438
1074	U.S. Patent No. 7,076,661
1075	U.S. Patent No. 6,771,657
1076	U.S. Patent No. 6,389,473
1077	U.S. Patent No. 6,662,329
1078	International Application Publication No. WO 2003/026220
1079	Trappe, “Key Management and Distribution for Secure Multimedia Multicast” (IEEE Dec. 2003)
1080	D. McGovern, “Pushing the internet direct to the user - security issues,” IEE Seminar on IP Over Satellite - The next Generation: MPLS, VPN and DRM Delivered Services, 2003., 2003, pp. 122-138, doi: 10.1049/ic:20030063.
1081	U.S. Patent No. 7,277,941
1082	Mike Knee, MPEG Video
1083	U.S. Patent No. 7,266,613
1084	U.S. Patent Application Publication No. 2004/0202320
1085	U.S. Patent No. 7,823,009
1086	U.S. Patent No. 8,098,819
1087	U.S. Patent Application Publication No. 2004/0236958
1088	International Application Publication No. WO 2001/015162
1089	U.S. Patent Application Publication No. 2004/0107356
1090	U.S. Patent No. 7,739,501
1091	U.S. Patent Application Publication No. 2004/0162871
1092	U.S. Patent Application Publication No. 2002/0129383
1093	U.S. Patent Application Publication No. 2004/0005061
1094	U.S. Patent Application Publication No. 2005/0160292
1095	U.S. Patent No. 6,959,086

Exhibit	Description
1096	RFC 3394: Advanced Encryption Standard (AES) key wrap algorithm
1097	U.S. Patent No. 7,257,227
1098	U.S. Patent No. 6,993,508
1099	Deposition of Aviel D. Rubin, Ph.D. (Dec. 12, 2024) (“Rubin-Depo.”)
1100	U.S. Patent Application Publication No. 2003/0140257
1101	U.S. Patent Application Publication No. 2004/0199771
1102	U.S. Patent Application Publication No. 2005/0177740
1103	U.S. Patent Application Publication No. 2004/0199667
1104	U.S. Patent Application Publication No. 2005/0050218
1105	U.S. Patent Application Publication No. 2003/0187799
1106	National Institute of Standards and Technology, NIST Special Publication 800-57, Recommendations for Key Management – Part 1: General (Aug. 2005)
1107	U.S. Patent Application Publication No. 2004/0236958
1108	U.S. Patent No. 6,169,843
1109	MPEG-2 - a tutorial introduction to the systems layer (IEEE 1995)
1110	U.S. Patent Application Publication No. 2003/0145329
1111	Reply Declaration of Samrat Bhattacharjee, Ph.D. (“Bhattacharjee-Reply”)
1112	U.S. Patent Application Publication No. 2004/0010699
1113	European Patent Application Publication No. EP1,564,686
1114	U.S. Patent Application Publication No. 2004/0010699
1115	U.S. Patent Application Publication No. 2004/0187014
1116	RESERVED
1117	U.S. Patent Application Publication No. 2006/0143350

I. GROUND 2: CLAIMS 1-10 ARE UNPATENTABLE OVER FOSTER-HAYHURST¹

Ground 2 combines Foster’s encryption methods with Hayhurst’s distributed-storage technique. Petition, 55-65. Foster divides a dataset (e.g., movie file) into segments, encrypts the segments with respective keys, encrypts those keys with a key-encryption key (KEK), and stores encrypted segments+keys on storage devices. Foster, [0005], [0040]-[0041], [0064]. Hayhurst, like Foster, “segments” a “media file (movie),” encrypts each segment, and then distributes segments to different storage devices. Hayhurst, [0006]-[0007]. Petitioner demonstrated POSAs would have utilized Hayhurst’s distributed-storage technique in Foster to reduce bandwidth requirements, add redundancy/backup, and increase security. Petition, 61-62.

SFI advances three counterarguments: (1) Hayhurst is not analogous art; (2) POSAs lacked motivation for Foster-Hayhurst; and (3) Foster-Hayhurst does not disclose *shares* and *data chunks*. SFI’s arguments fail.

¹ Emphases added; internal quotations, citations, and original alterations omitted.

A. Hayhurst is Analogous Art²

1. Hayhurst is in the patent's field of endeavor.

SFI argues “the ’854’s field is securing data,” including securely storing and communicating data. POR, 33-35. Hayhurst is in that field.

Hayhurst’s “**Technical Field**” is “the field of electronic media delivery...including the **secure handling and storage** of such media.” Hayhurst, [0002]. That alone should be dispositive that Hayhurst is analogous art. *In re Wood*, 599 F.2d 1032, 1036 (C.C.P.A. 1979). EX1111 (“Bhattacharjee-Reply”), ¶¶4-12.

Hayhurst’s specification reinforces that Hayhurst’s field is securing data. As the Board recognized, Hayhurst “provides **security** and deterrence” via its “segmented and distributed storage of the content.” DI, 21-22 (citing Hayhurst, [0008]); Hayhurst, [0021] (“[S]egmenting the movie [data] provides increased **security** from piracy....”). Hayhurst further enhances security because “segments are **each encrypted**...to prevent unauthorized viewing.” Hayhurst, [0007]. EX1099 (“Rubin-Depo.”), 108-109. Hayhurst’s technique provides additional “increased

² SFI suggests the Petition had to demonstrate that Hayhurst is analogous art (POR, 33), but a “petitioner is not required to anticipate and raise analogous art arguments in its petition.” *Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1379 (Fed. Cir. 2023).

security” because restoring the data also requires knowing “the correct method for recombining the segments,” which is “stored in a” secured file. Hayhurst, [0021]. EX1003 (“Bhattacharjee”), ¶¶178-181; Bhattacharjee-Reply, ¶¶13-16.

SFI says Hayhurst’s field is “decentralized media delivery.” POR, 35-36. But that is **how** Hayhurst provides “**security** and [] deterrence to piracy” of stored data. Hayhurst, [0008]; DI, 22 (Hayhurst “generates content segments **to secure the data.**”). The ’854 patent similarly secures data via “geographical separation of...storage facilities.” EX1001, 19:64-67; Bhattacharjee-Reply, ¶¶17-18³; Rubin-Depo., 126-135.

SFI’s assertion that Hayhurst is only “tangentially relate[d]” to securing data (POR, 36) is irreconcilable with Hayhurst **explicitly** saying its “Technical Field” includes “**secure** handling and storage of [] media.” Hayhurst, [0002]. Moreover, Hayhurst’s “segmented and distributed storage” of data is not tangential to securing data—it is **how** Hayhurst secures data to “**provide a high level of security.**” Hayhurst, [0008]. Bhattacharjee-Reply, ¶¶19-21.

³ The ’854 patent says its disclosures apply to “peer-to-peer file-sharing” and “video broadcasting,” two applications covered by Hayhurst’s teachings. EX1001, 81:40-50.

SFI argues Hayhurst does not teach that security was a problem “or that its invention addresses” that problem. POR, 36. But “the field-of-endeavor test does not look to the problem that the patent purports to address.” *Netflix, Inc. v. DivX, LLC*, 80 F.4th 1352, 1359 (Fed. Cir. 2023) (“It is enough that the prior art reference falls within the relevant field of endeavor of the patent-in-suit.”). Moreover, Hayhurst says its “approach” “provides **increased security**.” Hayhurst, [0021]. Thus, Hayhurst recognized “increased security” was needed and addressed that need. Bhattacharjee-Reply, ¶¶22-23.

SFI cites two cases: *Clay* and *Wang*. POR, 35-37. The persuasive value of these pre-*KSR* cases is questionable because *KSR* directs fact-finders to “construe the scope of analogous art broadly.” *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1238 (Fed. Cir. 2010).

Additionally, the cases are factually distinguishable. In *Clay*, **extracting crude** petroleum at **elevated** temperatures and pressures was a different field from **storing refined** liquid hydrocarbons at **ambient** temperature and pressure. 966 F.2d at 659. Contrary to what SFI says (POR, 37), those references were found **not** to be “similar.” *Id.* at 659-660. In *Wang*, the Federal Circuit found substantial evidence supported a jury’s presumed finding that “**compact** modular memories” and “memory circuits” of “**varying sizes**” were different fields. 993 F.2d at 864.

Significant technical distinctions like the above are absent here. As discussed, the '854 patent and Hayhurst describe overlapping techniques for securing data. Hayhurst **expressly** says its Technical Field “relates to” the “secure handling and storage” of data ([0002]) and does so using a technique the '854 patent itself says secures data, *i.e.*, distributed storage. Bhattacharjee-Reply, ¶¶24-26. Hayhurst is plainly within the '854 patent's field.

2. Hayhurst is reasonably pertinent to problems the '854 patent relates to.

The '854 patent identifies several problems that Hayhurst is reasonably pertinent to.

User-Independent Security. SFI only addresses the '854 patent's alleged problem of providing a “cryptographic system whose security is user independent.” POR, 38-39 (quoting EX2033, ¶106). Hayhurst is reasonably pertinent to that problem and addresses it by segmenting and distributing data without user action. Hayhurst, [0027] (cited Petition, 61, 65). As the Board correctly observed, users cannot undermine Hayhurst's security because “no one subscriber unit has more than one media segment, and a single segment has little value.” DI, 22; Hayhurst, [0021], [0027]-[0029]. Bhattacharjee-Reply, ¶¶27-36. Rubin-Depo., 115-120.

Computer-Network Security. Hayhurst is also reasonably pertinent to other problems the patent discusses. *In re Asset Guard Prods., Inc.*, 2022 WL 1097363, *4 (Fed. Cir. Apr. 13, 2022) (prior art need only be reasonably pertinent to *a* problem

the patent relates to, not its “central” problem). The patent identifies the problem of “ensuring [that] data stored and transmitted over” “computer networks” “cannot be read or otherwise compromised.” EX1001, 1:30-39; Rubin-Depo., 109-110. Hayhurst similarly addresses problems “relat[ing] to...**electronic** media **delivery**...including the **secure handling and storage** of” data ([0002]) and “deter[ing] [] piracy” ([0008]). Bhattacharjee-Reply, ¶¶37-39.

Distributed Storage. The patent splits and “stor[es]...data in geographically remote secure data storage facilities.” EX1001, 5:53-56. It does that to address problems with “protecting...against compromise of any individual data storage facility” (5:53-56) and data “remain[ing] whole and intact and subject to attack” (56:47-50). POR, 68-69 (admitting the patent has these “concern[s],” and addresses them by “splitting the data set into shares”). Hayhurst’s distributed-storage technique addresses those problems and solves them in the same way. *Supra* §I.A.1. Rubin-Depo., 124-135; Bhattacharjee-Reply, ¶¶40-47.

B. POSAs Had Motivation For Foster-Hayhurst

The Petition established POSAs had reason to implement Foster’s system using Hayhurst’s distributed-storage technique because it would, e.g., reduce a content provider’s bandwidth requirements and increase security by storing portions of a *data set* in different storage devices. Petition, 61-65.

In response, SFI argues Hayhurst’s distributed-storage technique is incompatible with Foster’s goal of “avoiding delays” for “streaming live television.” POR, 42. But Foster must be “read for **all** that it teaches.” *In re Mouttet*, 686 F.3d 1322, 1331 (Fed. Cir. 2012). Foster’s teachings are not limited to live-streaming, as Foster teaches **storing** encrypting content for and by recipient(s) (*e.g.*, video-on-demand). Foster, [0064]. In (at least) Foster’s storage context—relied upon in the Petition (65, 80-82)—POSAs would have recognized the benefits of combining Foster with Hayhurst. Bhattacharjee-Reply, ¶¶48-57.

1. Foster stores encrypted content.

SFI argues Foster’s “fundamental goal” is “synchronization” (POR, 42-43), but SFI improperly limits Foster’s synchronization to live-streaming applications. Foster teaches that attaching an encryption key to encrypted data is a form of “synchronization,” which may reduce (i) the risk of applying the wrong key to the wrong chunk of data and (ii) the time needed to locate the correct key for a chunk of data. Petition, 55-57 (citing Foster, [0004]-[0007]); Foster, [0002]-[0007]; Bhattacharjee-Reply, ¶58.

SFI argues Foster uses “synchronization” to “reduc[e] delays in viewer access to content **as it is transmitted**” in real-time. POR, 42-43 (citing Foster, [0008]). But the same sentence SFI cites also teaches that Foster attaches a key to encrypted data “for synchronized...**storage**.” Foster, [0008]. Foster repeatedly says

synchronization improves data for “transmission...**or storage**.” Foster, Abstract; *see also* [0007]-[0008], [0048], [0064], [0079], claim 11. The Board recognized this at institution. DI, 17 (Foster “synchronously **stor[es]** the encrypted content”). SFI admitted in IPR2024-00214 (Paper 22, 44, 51) that Foster “**teaches**...the ‘recipient 430 **can**....**store** the encrypted content.’” Similarly, SFI’s expert admitted Foster’s “recipients can determine whether to **store**.” Rubin-Depo., 187-191 (“The recipient...could decide to **store** it.”); EX2033, ¶140 (“Foster’s system focuses upon,” *e.g.*, “content **stored** on a DVD”). That Foster stores its encrypted data should not be genuinely disputed.

Foster recognizes that synchronization reduces latency for storage-based purposes, like for Digital Rights Management Systems (“DRMSs”). Foster, [0064] (“[A] recipient will receive or **store** encrypted content...”). Rubin-Depo., 83-85, 96-99. In Foster’s DRMS, “content is packaged and **loaded** [i.e., stored] onto a web server” and subsequently “**downloaded to** [i.e., stored to a] personal computer” for on-demand access (i.e., viewing stored content whenever the user wants to). Foster, [0005], [0049] (users access “content on [the] media server”); FIG. 1 (content is “stream[ed] **or stored**”); EX2039, 6-10 (DRMS “safeguards **content** when **at rest** [i.e., stored],” and when “**stored** on a receiving device”). Foster’s synchronization also facilitates “random access” to stored chunks of “protected content” (*e.g.*,

starting a stored movie at any point). Foster, [0005], [0064] (random access is “access[ing] and decrypt[ing]...**at any packet**”). Bhattacharjee-Reply, ¶¶59-66.

Consistent with its DRMS disclosures, Foster discloses processing datasets for an MPEG “program stream,” which Foster says (and POSAs knew) is intended for storing “**in fixed storage**.” Foster, [0073]; *see also* EX2014, 1 (“[p]rogram streams are **designed for...storage**”); EX1108, 1:65-2:31; EX1109, 1-9, 13); EX1072, [0002]-[0004], [0011], [0042]-[0043]; Bhattacharjee-Reply, ¶¶67-73; Rubin-Depo., 82-85 (admitting there are “different ways of encoding MPEG data” but he did not “discuss[] the distinctions”). Foster’s text makes clear that Foster includes storage-based embodiments.

Finally, even Foster’s implementation in conditional-access systems (“CASs”) is not limited to “live” broadcasting. POSAs knew content service providers used CAS in video-on-demand (VOD), like Foster describes ([0005], [0049]-[0052]). In VOD systems, “content **is stored pre-encrypted** on hard drives in the VOD server” (EX1110, [0007]) and again in “**storage** media in which the delivered **content can be stored**” (EX1072, [0043]). Bhattacharjee-Reply, ¶¶74-85 (citing EX1073, [0001]-[0004], [0043], [0098], FIG. 3; EX1097, 2:31-53, FIG. 1; EX1075, 1:51-67, FIG. 2; EX1076, 9:53-10:5, FIG. 2; EX1077, 1:12-21, 1:48-65, 3:56-5:8, FIG. 1; EX1092, [0079]).

At deposition, SFI's expert admitted POSAs knew CAS was "used in a lot of places," like "[f]ile systems," "**video-on-demand**," "basically **any place...you want to prevent people who aren't authorized** from getting to something." Rubin-Depo., 85-86, 87-89 (admitting with VOD "content producers [] would license the content to the [VOD] hosting sites"; "service providers [] would keep the content" that "would be **stored**," for example, "[o]n a server"), 90-94 (VOD's "intermediaries" "house the actual content"). Foster-Hayhurst is consistent with Foster's disclosure of storing content for various purposes. Petition, 61-63; Bhattacharjee-Reply, ¶¶86-88.

2. Foster-Hayhurst is consistent with Foster's goals.

Relying on its narrow interpretation of Foster as limited to streaming live broadcasts, SFI argues Hayhurst's distributed-storage technique would "thwart Foster's goals, make Foster inoperable for its intended [streaming] purpose, and compromise any security benefits otherwise provided by Foster alone." POR, 51-61. These critiques lack merit.

SFI's first two critiques depend on narrowly interpreting Foster as being concerned **only** with real-time video-streaming, *e.g.*, live events. POR, 52-58 ("Foster seeks to securely stream content, *e.g.*, live television, without [] delay..."). But as discussed above (§I.B.1), Foster is not so limited and also concerns **storing** secured data. *E.g.*, Foster, [0007]-[0008].

SFI speculates Foster-Hayhurst would have excessive delays when a movie file is distributed amongst “thousands” of recipients. POR, 52-55. But Hayhurst’s distributed system **reduces** delays by increasing aggregate speed and efficiency of content delivery by having multiple devices storing and delivering data. Petition, 74 (citing corroboration); Bhattacharjee-Reply, ¶¶89-105; Rubin-Depo., 89-93.

SFI’s third critique—that Foster-Hayhurst makes Foster less secure—improperly considers the references individually and is premised on the mistaken idea that (i) changing/replacing the key-encryption-key (KEK) as discussed in Foster is required in Foster-Hayhurst **and** would be more difficult if the KEK were stored in multiple locations, and (ii) storing the KEK in more locations makes it more vulnerable. POR, 58-61.

SFI cites Foster, [0053]-[0054] but that only says Foster’s key “**can** be re-encrypted with a different” KEK. Contrary to SFI’s arguments (POR, 59), Foster does not **require** changing the KEK. Rather, Foster recognizes “re-encrypting the content itself,” rather than changing the KEK, is an alternative. Foster, [0053]-[0054]. Bhattacharjee-Reply, ¶¶106-109.

Moreover, POSAs knew changing a KEK in Foster-Hayhurst would be comparable to doing so in Foster alone because both would involve changing a KEK used for multiple segments. Furthermore, POSAs knew how to change/replace

KEKs across many devices/users. Bhattacharjee-Reply, ¶¶104-105, ¶¶110-115 (citing EX1078, 4:5-28; EX1079, 544-546; EX1080, 2-7).

Regardless, Foster-Hayhurst would not store a KEK on user devices. As in Foster alone, users could only access a KEK once authorized to decrypt the content. Foster, [0049], [0052]. Based on Hayhurst's teachings, the "encryption key to unlock the movie" (Foster-Hayhurst's KEK) would be stored on the "main server," not at each subscriber. Hayhurst, [0007] (cited Petition, 59), [0021]. Bhattacharjee, ¶188 (Foster-Hayhurst's KEK is "**maintained in a storage device...until requested by a subscriber....**") (cited Petition, 64-65); Bhattacharjee-Reply, ¶¶116-117.

Moreover, independent of where the KEK is stored, Foster-Hayhurst would still reduce the risk of unauthorized access compared to Foster because an attacker must collect chunks from Foster-Hayhurst's multiple storage devices, rather than from one storage device, as in Foster. Petition, 59-60 (citing Hayhurst, [0005], [0008]); Bhattacharjee-Reply, ¶¶118-119.

Thus, Foster-Hayhurst does not diminish Foster's security. *Contra* POR, 58. Rather, Hayhurst adds "**a high level of security.**" Hayhurst, [0008]. Bhattacharjee-Reply, ¶¶118-120; Rubin-Depo., 124-126.

Even if Foster-Hayhurst were reducing security in ways SFI alleges, Foster-Hayhurst was still obvious because it added (1) the security provided by Hayhurst's

distributed storage **and** (2) speed/efficiency/redundancy benefits. Petition, 61-63 (citing corroboration); Bhattacharjee-Reply, ¶¶121-125 (citing EX1081, 15:6-25); Rubin-Depo., 90-93, 134-137. *Corephotonics, Ltd. v. Apple Inc.*, 2021 WL 4944471, at *6 (Fed. Cir. Oct. 25, 2021) (“design decisions entail making tradeoffs among multiple objectives”).

SFI argues “Foster’s system has no need for redundancy” (because Foster “can simply resend dropped packets”) or “for efficiency/intelligence when sending on a one-to-one basis.” POR, 62. But Foster-Hayhurst’s redundancy – storing identical *chunks* at multiple locations – addresses known problems from Foster’s storing and delivering content on a one-to-one basis (e.g., power/network failure at the one source). Rubin-Depo., 135-137. Similarly, efficiency/intelligence allows for, e.g., selecting data source(s) closer to the destination, to deliver content faster/more efficiently than one source could typically achieve. Rubin-Depo., 89-92. EX1001, 69:56-58; Bhattacharjee-Reply, ¶¶126-129.

C. Foster-Hayhurst Has *Data Chunks*

Claim 1 requires “*distributing [a] data set into a plurality of shares*” and encrypting shares, which the claim calls ***data chunks***. SFI acknowledges Petitioner “map[ped] the claimed ‘plurality of shares’ to Foster’s” “MPEG packet payloads, [*i.e.*, content units],” the “‘data chunks to Foster’s encrypted content units..., and” “the ‘data set’ to Foster’s content.” POR, 63-65 (citing, *inter alia*, Petition, 72-74).

SFI argues Foster’s MPEG payloads are not *shares* and encrypted content units (comprising payloads) are not *data chunks*. POR, 63. The Board should (again – DI, 20-22) reject SFI’s argument because nothing in the intrinsic record supports SFI’s narrow interpretations of *share/data chunk*.

SFI says the Petition “is conclusory” for not explaining “what ‘data chunks’ or ‘data shares’ are or why [Foster’s] packet ‘payloads’ are ‘data shares’ (or ‘data chunks’ when encrypted).” POR, 66; POPR, 42. But neither party construed those terms because their meanings are readily apparent. *See* EX1064-EX1065; *Axonics, Inc. v. Medtronic, Inc.*, 75 F.4th 1374, 1380-81 (Fed. Cir. 2023).

Claim 1’s plain language provides that a *data set* is the set of data to be securely stored, a *share* is a portion (or less than all) of that *data set*, and a *data chunk* is an encrypted *share*. At deposition, SFI’s expert acknowledged that “the share is the thing that something gets split into” (Rubin-Depo., 17) and similarly that the terms *share/chunk* just “refer[] to the pieces that have been split off from the original data set” (Rubin-Depo., 157-158). Foster’s payloads are exactly that because each payload’s data is a split portion of the complete *data set* being secured by Foster. Bhattacharjee-Reply, ¶¶130-133.

The 854’s specification places no limit on the relationship between a *data set* and *share*. Instead, the specification says POSAs “will recognize...a wide number of alternatives for the data splitting process,” and that “data may be split into any

desired” “size unit.” 21:9-25; 15:51-16:3 (similar), 21:27-37 (similar), 74:56-75:10 (“any other suitable parsing and splitting approach may be used to generate portions of data from an original data set”). The patent explicitly allows *shares* to take any form so long as they are a subset of the *data set*. Rubin-Depo., 156-158. Bhattacharjee-Reply, ¶¶134-139.

SFI suggests a *share* must be “cryptographically generated” so the splitting of the *data set* by itself makes it less susceptible to “attack.” POR, 68-69. But the specification says “data units may be distributed into” shares in different ways, including simply “**fixed** or predetermined data unit size”; “randomly generated data unit size” is **optional**. EX1001, 21:33-37. Moreover, dependent claims 4-6 limit claim 1’s *shares* to being generated using a “random technique.” That confirms that the independent claim is broader and not limited to generating *shares* using particular techniques that might further increase security. *Voda v. Cordis Corp.*, 536 F.3d 1311, 1320 (Fed. Cir. 2008). Bhattacharjee-Reply, ¶¶140-148.

Furthermore, Foster’s payloads “are generated to further secure the data” (POR, 68-69), because each is encrypted with a different key to “provide **enhanced security**” (Foster, [0004], [0071]). Bhattacharjee-Reply, ¶147.

That Foster calls its subsets of data “payloads” rather than *shares* (POR, 66) is immaterial because the prior art “does not need” to “us[e] the same words as the patentee.” *Teva Pharm. Indus. Ltd. v. AstraZeneca Pharms. LP*, 661 F.3d 1378,

1384 (Fed. Cir. 2011). SFI does not dispute that Foster’s payloads (in content units) each comprise less than all the data of Foster’s content file (*data set*). That is all that the claimed *shares* require.

It is also irrelevant that some non-prior-art “literature” says a “payload” or “packet” can be “divided into ‘chunks’ or ‘shares.’” POR, 66.⁴ As discussed, neither the challenged claims nor the specification preclude a payload packet from (i) being a single *share* (or *chunk* when encrypted) or (ii) being divisible into multiple *shares/chunks*. The patent only requires that a *share* contain less than the entire *data set*. Foster’s payloads are each less than Foster’s entire *data set*. Bhattacharjee-Reply, ¶¶149-156.

GROUND 1: CLAIMS 1-10 ARE UNPATENTABLE OVER ORSINI

For Ground 1, SFI only disputes limitation [1C]: “*an encryption operation based on the external key to further secure...data chunks.*”

Petitioner advanced several alternative arguments demonstrating how Orsini discloses and renders obvious [1C]. Petition, 32-45. At institution, the Board preliminarily found those arguments unpersuasive. DI, 25-39.

⁴ Other literature says a packet can contain a chunk. EX1082, 8; EX1083, 7:32-40; EX1084, [0026]; EX1085, 4:7-25.

While Petitioner believes its arguments have merit, Petitioner below focuses on one obviousness argument to simplify the trial. Specifically, Petitioner’s argument that POSAs would have encrypted Orsini’s share keys with a key-encryption-key (“KEK”) to safeguard the share keys from detection, a technique that **multiple** corroborating references demonstrate was known and desirable in the art. Petition, 43-45 (citing corroboration).

SFI does not dispute that encrypting encryption keys with KEKs was known or that encrypting Orsini’s share keys with a KEK meets [1C] under SFI’s claim constructions. POSAs would have used that known technique in Orsini because, as even SFI’s expert admits, POSAs would “not put [] security in anything other than the keys” and the way Orsini allegedly protects its share keys – by obfuscating which *data chunk* each key is stored with – “is not putting the protection in the keys, so...this **does not on its own provide security.**” Rubin-Depo., 155. The expert’s candid admission is consistent with the Petition’s prior-art evidence explaining that “[s]ecurity’ comes from ‘encrypt[ing] the encryption keys themselves’ with ‘a key encryption key.’” Petition, 43 (quoting EX1036). On the fully developed record, [1C] is plainly obvious over Orsini.

D. POSAs Would Have Encrypted Orsini’s Share Keys Using a Conventional KEK

The parties agree Orsini’s Figure 21 results in an encrypted *share* of data being stored with a plaintext (non-encrypted) share-encryption key. Petition, 43-45;

POR, 2, 21-23. Each non-encrypted share key that is stored with an encrypted share is not the key to unlock that share, but even SFI recognizes that an attacker nonetheless can “reconstruct [Orsini’s] dataset if the attacker has access to each of the shares,” because Orsini’s share keys are not encrypted. POR, 4; EX2033, ¶41.

The Petition demonstrated, supported by expert testimony **and multiple pieces of corroborating evidence**, that POSAs would have encrypted Orsini’s keys with a KEK to prevent an attacker from reconstructing the encrypted dataset, even when they possessed every encrypted share. Petition, 43-44. The Petition’s corroborating evidence was direct in its teaching: “cryptographic keys should **never** occur in clear [*i.e.*, unencrypted] form outside the cryptographic device.” EX1035, 12:15-23 (cited Petition, 43).

Petitioner’s cited prior art explains that POSAs knew that when an encryption key is transmitted or stored (as in Orsini), the system should “encrypt the encryption keys themselves...[with] a key encryption key” EX1036, 1:66-2:6 (cited Petition, 43). That was true whether the “encryption keys were included with the encrypted message” (*id.*) or stored separately from and/or obfuscated with encrypted data-
portions (EX1035, 10:42-62; EX1036, 1:66-2:6; EX1086, 7:3-22; EX1087, [0017]-[0025]; EX1112, [0022]-[0027] (“Wherever the session key is stored, it is preferable that it is encrypted beforehand.”). Petition, 43-45. Bhattacharjee-Reply, ¶¶157-179.

POSAs, therefore, would have recognized that Orsini's obfuscation provides (negligible) non-cryptographic security that depended heavily on the attacker not possessing the shares. Conversely, POSAs would have recognized that encrypting Orsini's keys with a KEK provided cryptographic (stronger) security, whose protection would have continued **even when** all encrypted shares were obtained (unlike Orsini's obfuscation). Bhattacharjee, ¶¶131-134; Bhattacharjee-Reply, ¶¶180-188. EX1100, [0010]. Rubin-Depo., 137-147, 150-156.

Put simply, POSAs knew leaving Orsini's keys unencrypted was undesirable because, even with Orsini's obfuscation, the keys (and thus the shares/chunks they unlocked) remained exposed and subject to an attack that a KEK would have prevented.⁵ EX1003, ¶132; Bhattacharjee-Reply, ¶¶189-193 (citing EX1106).

Therefore, encrypting Orsini's share keys with a KEK was obvious because it entailed using POSAs' ordinary skill to perform a known technique (encrypting encryption keys) to solve a known problem (protecting encryption keys from discovery), with a reasonable expectation of success and no unexpected results. *Intel*

⁵ The Board, when instituting IPR against the related '116 patent, recognized that POSAs knew KEKs beneficially "provided even further security" in systems (like Orsini's) that store encrypted data portions with unencrypted keys of other data portions. IPR2024-00212, Paper 11, 17.

Corp. v. PACT XPP Schweiz AG, 61 F.4th 1373, 1379-81 (Fed. Cir. 2023) (obvious to use alternative, known technique in a reference that “already address[ed] the same problem” in a different way). That motivation-to-combine theory was well-reasoned and well-supported.

1. The Board Misunderstood the Petition’s Obviousness Argument.

At institution, the Board said the “reasoning” behind the Petition’s KEK-based obviousness argument was the same reasoning supporting the Petition’s argument that Orsini’s public-key disclosures meet [1C]. DI, 38-39. The Board found the public-key encryption anticipation argument improperly combined distinct Orsini embodiments. *Compare* DI, 34 (“[T]he public key is not shown in Figure 21....Rather, Petitioner combines the features from multiple embodiments to arrive at the claimed invention.”) *with* DI, 38-39 (similar critique).

Respectfully, however, the reasoning behind Petitioner’s anticipation argument and the reasoning (and evidence) behind Petitioner’s KEK-based obviousness argument are different. The anticipation argument was premised on Orsini’s disclosures of using public-key encryption. Petition, 38-39. The KEK-based obviousness argument was premised on using a conventional, non-public-key KEK to encrypt Orsini’s share keys, based on POSAs’ corroborated background knowledge that encryption keys—like Orsini’s share keys—“**should never**”

(EX1035, 12:15-23) be electronically stored/transmitted in unencrypted fashion. *Compare* Petition, 43-45 *with* 38-39. Bhattacharjee-Reply, ¶¶198-199.

In preliminarily rejecting that obviousness argument, the Board did not mention, much less discuss, the Petition’s evidence of POSAs’ background knowledge or Dr. Bhattacharjee’s related testimony. DI, 38-39. Respectfully, the Board must consider Petitioner’s evidence. *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2012).

2. Petitioner Does Not Rely on Common Sense To Supply a Missing Limitation.

SFI argues the Petition’s KEK-based obviousness argument impermissibly relies on common sense to supply a missing limitation. POR, 18-21. This is incorrect.

[1C] is not missing in the prior art. As discussed *supra* §II.A, the Petition cited EX1035’s **and** EX1036’s disclosures of the known desirability of using a KEK to encrypt an encryption key for storage. Petition, 43; *see infra* §II.A.3. As the Board found, Foster also discloses [1C]. DI, 13, 24. Other references also teach using KEKs to encrypt keys that encrypt “partitions[s]” of “digital content.” EX1088, 2:20-3:16; *see also* EX1080, 2-7; EX1106, 34, 61, 123-125. Bhattacharjee-Reply, ¶¶200-210.

Moreover, the Petition did not rely on only “common sense.” The Petition provided reasoned analysis — supported by multiple pieces of corroborating

evidence and expert testimony — detailing why POSAs would further secure Orsini’s share keys using the well-known (not SFI-invented) technique of encrypting encryption keys. *Bhattacharjee-Reply*, ¶¶211-214.

The Federal Circuit has explained that *Arendi* and *DSS* (cited POR, 19-20) do not preclude obviousness based on different teachings in the art to meet different elements of a claim limitation. *E.g.*, *Fleming v. Cirrus Design Corp.*, 28 F.4th 1214, 1222 (Fed. Cir. 2022) (“That the proposed *combination*...—rather than one of the individual references—discloses the disputed claim limitations does not defeat...obviousness.”) (emphasis original); *Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1339 (Fed. Cir. 2020) (obviousness is not based on “common sense” alone when supported by “corroborated” “expert evidence,” establishing that the limitation “was not only in the prior art, but also within the general knowledge of” POSAs).

3. SFI’s Challenges to Petitioner’s Motivation-to-Combine Theory Fail.

SFI offers three challenges to Petitioner’s motivation-to-combine theory: (1) Orsini already provides sufficient security, (2) KEK-based encryption introduces complications, and (3) the modification is hindsight driven. Each argument fails.

a. POSAs Would Have Wanted to Increase Orsini's Security.

SFI argues POSAs would not further secure Orsini's system because Orsini itself was satisfied with its security. POR, 21-24. SFI's argument misunderstands how POSAs would read Orsini and the law of obviousness.

Orsini's use of **non**-cryptographic obfuscation—storing a share key with another share—confirms that Orsini itself recognized a need to further secure its keys. But POSAs knew that Orsini's non-cryptographic obfuscation technique was **less secure** than **also** (or alternatively) encrypting Orsini's share keys using a conventional KEK because, unlike Orsini's obfuscation, a KEK would **cryptographically** protect share keys, even when all shares were collected. Bhattacharjee-Reply, ¶¶215-222; EX1089, [0569]; EX1090, 2:39-41 (“The more difficult it is for an unauthorized entity to obtain a valid key, the more secure the cryptographic scheme.”). SFI does not – because it cannot – dispute that encrypting Orsini's share keys would make Orsini more secure.

Orsini's Figure 21 divides data into four shares/chunks and stores share keys with those shares/chunks. Orsini, [0298]-[0301]. That allows (at most) twenty-four different chunk-key pairings. Rubin-Depo., 25. POSAs understood that computers could easily overcome Orsini's obfuscation by trying all twenty-four possibilities until identifying the correct one. Bhattacharjee-Reply, ¶¶223-225; Rubin-Depo., 22-25, 154-156; EX2007, 11 (even “26 possible keys” is subject to “a *brute-force*

attack,” but “any secure encryption **must not be vulnerable to such brute-force attack**”) (italicized original).

Even SFI’s expert admitted that describing Orsini’s different combinations “is a pretty simple math problem” because “it wouldn’t take long” even to write out the combinations by hand. Rubin-Depo., 22-25, 154-156 (“I **don’t** even **think it’s really involving a lot of math**. You’re just putting something with other things and not putting it with other things....[P]erforming an **obfuscation is [] not putting the protection in the keys**, so I would say **this does not on its own provide security....[Y]ou should put your security in the keys** and not in the hiding of your algorithms.”).

Orsini’s obfuscation was also contrary to industry-wide best practices. For example, the U.S. Government’s National Institute of Standards and Technology (“NIST”) directed POSAs that when, as in Orsini, a “key exists external to the cryptomodule, **confidentiality protection shall be provided either by encryption (e.g., key wrapping) [*i.e.*, a KEK]**” or physically protecting keys. EX1106, 34, 61, 124-125.⁶ Bhattacharjee-Reply, ¶¶189-193.

⁶ **Physically** securing plaintext key information (e.g., in a safe) would be contrary to Orsini’s **electronic** storing of encrypted data with keys.

Thus, SFI's assertion that Orsini's non-cryptographic obfuscation "achieves the benefit...served by" a KEK's cryptographic protection (POR, 23) is incorrect. Bhattacharjee-Reply, ¶226; Rubin-Depo., 22-25, 154-156.

Moreover, even if SFI were correct that Orsini teaches that its obfuscation was sometimes "sufficient" to protect some *data sets* (POR, 24), that would not make using the known KEK technique non-obvious in Orsini's system for all *data sets* and/or risk levels. Rubin-Depo., 113-115. *Cole Kepro Int'l, LLC v. VSR Indus., Inc.*, 2017 WL 2627982, *3 (Fed. Cir. 2017) (that a prior art reference discloses a certain level of a solution to a problem "does not discourage," by that fact alone, seeking a greater level of solution to the same problem). Bhattacharjee-Reply, ¶¶227-229. Rubin-Depo., 145-147 ("in security you want to provide defense in depth, meaning **the more layers of security you have, the better**"; testifying that the '854 patent "talks about a multilayer encryption scheme" at EX1001, 65:61, which is Orsini, [0423]).

b. The Alleged Drawbacks to KEKs Were Easily Overcome and Are Legally Irrelevant.

SFI argues "drawbacks associated with managing and securing" KEKs would have dissuaded POSAs from using KEKs in Orsini. POR, 26-32. But SFI does not allege that addressing these alleged "drawbacks" was beyond POSAs' skill.

Orsini **already** taught techniques for managing and securing other KEKs, or (at least) could have been modified in a simple, straightforward way to use

conventional techniques for doing so. As discussed below (§II.B), Orsini supports prior art “Triple DES and AES” (Orsini, [0378]), which used and managed KEKs. Bhattacharjee-Reply, ¶¶230-232. Orsini also supports “a wide number of alternative key management systems.” Orsini, [0107].

Petition-cited prior art demonstrates that using/managing KEKs was conventional. Petition, 43 (citing EX1035-EX1036). For example, EX1036 discloses a “system for **managing keys**,” including KEKs (2:29-61) and says the “prior art” already included “security infrastructure to solve the key management problem[]” (2:7-22). *See also* EX2032, 683-84 (describing “key management” for “KEKs”); EX1017, 1:50-1:68 (similar); EX1093, [0013], [0035]-[0039] (similar), [0057]-[0060]. As discussed above (§II.A.3.a), the U.S. Government (NIST) urged POSAs to use KEKs and discussed the development of related key-management systems. EX1106, 5, 34-36, 61, 72, 123-125. The evidence is clear that any alleged “drawbacks” to managing KEKs were not beyond POSAs’ skill (at most involving known tradeoffs), and thus do not defeat obviousness. *Intel*, 61 F.4th at 1381; Rubin-Depo., 185-186.

Even if the alleged “drawbacks” to KEKs that SFI identifies were true, that would still not defeat the obviousness of using this known technique. SFI does not dispute that using the known KEK technique in Orsini’s system would have increased security because Orsini stores its share keys in unencrypted form, which

prior art taught “should **never** occur” for security reasons. EX1035, 12:15-23; Bhattacharjee-Reply, ¶¶233-238.

POSAs also knew that securing data often involves tradeoffs in “convenience and security, speed,” etc. EX1081, 15:6-25; Bhattacharjee-Reply, ¶¶239-240.

Thus, even if encrypting Orsini’s share keys with a KEK added complexity, that would not defeat obviousness because it “does not show that [using KEKs] was unknown or could not have practical applications.” *In re Cree, Inc.*, 818 F.3d 694, 700-01 (Fed. Cir. 2016); *Corephotonics*, 2021 WL 4944471, at *6.

Encrypting Orsini’s share keys was not beyond POSAs’ “capability” and was nothing more than using a “known technique [KEKs] to address a known problem [the risk of storing an unencrypted encryption key outside the cryptographic device] using prior art elements according to their established function” and thus was obvious. *CyWee Grp. Ltd. v. ZTE (USA), Inc.*, 90 F.4th 1358, 1366 (Fed. Cir. 2024) (cleaned up).

c. Petitioner’s Motivation-to-Combine Theory Is Not Based on Hindsight, It Is Grounded in Evidence.

SFI contends the Petition’s KEK-based obviousness argument is driven by hindsight. POR, 29-32. This is plainly incorrect.

The Petition’s combination provides a specific motivation—supported by multiple pieces of **corroborating evidence** and Petitioner’s expert—to use a KEK for its known purpose and benefit of cryptographically securing encryption keys

being transmitted/stored outside the cryptographic device, rather than leave them unencrypted. Petition, 43 (citing **EX1035**, 12:15-23, 10:42-62; **EX1036**, 1:66-2:6; Bhattacharjee, ¶132); *supra* §II.A. That motivation-to-combine theory is grounded in evidence and reasoning, not hindsight. Again, Orsini **itself** recognized a need to protect its keys, but elected non-cryptographic obfuscation, rather a conventional, cryptographic KEK technique. Bhattacharjee-Reply, ¶¶241-242.

E. SFI’s Reasonable Expectation of Success Challenge Fails

SFI asserts POSAs had no “reasonable expectation of success in modifying Orsini to achieve claim 1.” POR, 4. But SFI never argues any specific reason **why** POSAs allegedly would not have reasonably expected success in using a KEK to encrypt encryption keys (like Orsini’s) as was known in the art, let alone submit evidence to substantiate any such unexplained reason. Bhattacharjee-Reply, ¶¶243-244; Petition, 44-45; Bhattacharjee, ¶134.⁷

As discussed above (§II.A.3.b), using KEKs and related key-management systems were known. Orsini encrypts shares using “Triple DES and AES” standardized techniques (Orsini, [0378]), which taught to encrypt their keys with

⁷ *Google LLC v. Nobots LLC*, IPR2022-00940, Paper 38, 38 (Nov. 23, 2023)

(“present[ing] additional evidence” “directed specifically to arguments” in POR challenging POSAs’ expectation of success is proper).

KEKs, and relied on existing key-management concepts. Bhattacharjee-Reply, ¶¶245-254; EX1017, 1:50-68; EX1094, [0056]-[0057] (“Triple-DES Key Wrap”); EX1090, 19:47-61, 21:1-22:54 (“AES[] key wrapping function”); EX1095, 1:32-47 (“key managements schemes are built on **commonly used**...concepts, such as key wrapping”), 3:10-15; EX1096, 1-3. Bhattacharjee, ¶¶93, 131-134; Bhattacharjee-Reply, ¶¶255-256.

Implementing the proposed modification was within POSAs’ capabilities.

Dated: 12-23-2024

Respectfully submitted,

/Gregory Nieberg/

Gregory Nieberg, Reg. #57,063

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned certifies that the foregoing **PETITIONER'S REPLY** contains 5,600 words excluding; a table of contents, a table of authorities, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: December 23, 2024

/Dara Del Rosario/

Dara Del Rosario

Paralegal

WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6 (e)(4)

I certify that on December 23, 2024, I will cause a copy of the foregoing document, including any exhibits filed therewith, to be served via electronic mail, as previously consented to by Patent Owner, upon the following:

Stephen J. Elliott

elliotts@sullcrom.com

Kenneth Weatherwax

Weatherwax@lowensteinweatherwax.com

Nathan Lowenstein

Lowenstein@lowensteinweatherwax.com

Colette Woo

Woo@lowensteinweatherwax.com

Dustin F. Guzior

guziord@sullcrom.com

Andrei Iancu

iancua@sullcrom.com

SFI_PTAB@sullcrom.com

Date: December 23, 2024

/Dara Del Rosario/

Dara Del Rosario

Paralegal

WOLF, GREENFIELD & SACKS, P.C.