

Filed on behalf of Petitioner by:

Paper No. ____

Elisabeth H. Hunt, Reg. No. 67,336
Richard F. Giunta, Reg. No. 36,149
Marc S. Johannes, Reg. No. 64,978
Gregory S. Nieberg, Reg. No. 57,063
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. IPR2024-00212
Patent No. 11,178,116

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	GROUND 1: TAJIMA	1
A.	Tajima’s Key Information Includes the Key	1
1.	Petitioner Did Not Rely On Inherency	2
2.	POSAs Understood Tajima’s Key Information Includes the Key	3
3.	SFI’s Allegations About What Key Information Means Fail	4
4.	SFI Does Not Dispute That Tajima’s Claims Disclose That “Key Information” Includes the Key	6
B.	Including Tajima’s Key in Tajima’s Key Information Was Also Obvious.....	8
C.	SFI’s Lack-of-Motivation Argument Fails.....	11
II.	GROUND 2: TAJIMA-FOSTER	12
A.	Even if Tajima’s and Foster’s Fields/Problems Were Different, Their Combination Was Still Obvious	13
B.	It Would Have Been Obvious to Encrypt Tajima’s Encryption Keys Using the Known KEK-technique and Store the Encrypted Keys With Data Fragments.....	14
1.	Tajima’s and Foster’s Alleged “Lack of Critical Disclosures” Do Not “Preclude Their Combination”	14
2.	Encrypting Tajima’s Keys Would Have Further Secured Tajima’s Data	16
3.	Foster Supports, Rather Than Discourages, Tajima-Foster	17
4.	Petitioner Demonstrated a Reasonable Expectation of Success in Implementing Tajima-Foster.....	19
III.	GROUND 3: TAJIMA-RIVEST	19
IV.	GROUND 4: TAJIMA-RIVEST-SHYU	20
V.	GROUND 5: FOSTER-HAYHURST	21
A.	Hayhurst is Analogous Art	21
1.	Hayhurst Has the Same Field of Endeavor.	21
2.	Hayhurst is Reasonably Pertinent to a ’116-Identified Problem.	22

B. POSAs Had Motivation For Foster-Hayhurst	24
1. Foster Stores Encrypted Content.....	24
2. Foster-Hayhurst Is Consistent With Foster’s Goals.....	26
C. Foster’s Payloads Are “ <i>Data Chunks</i> ”	29

TABLE OF AUTHORITIES

CASES

<i>ArthroCare Corp. v. Smith & Nephew, Inc.</i> , 406 F.3d 1365 (Fed. Cir. 2005)	2
<i>AstraZeneca AB v. Mylan Pharm. Inc.</i> , 19 F.4th 1325 (Fed. Cir. 2021)	18
<i>Cole Kepro Int’l, LLC v. VSR Indus., Inc.</i> , 695 F. App’x 566 (Fed. Cir. 2017)	17
<i>Corephotonics, Ltd. v. Apple Inc.</i> , No. 2020-1961, 2021 WL 4944471 (Fed. Cir. Oct. 25, 2021)	29
<i>DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.</i> , 567 F.3d 1314 (Fed. Cir. 2009)	18
<i>DSS Tech. Mgm’t v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	11
<i>Ex Parte Richard Kane</i> , APPEAL 2016-005068, 2018 WL 2332503 (May 14, 2018)	18
<i>In re Asset Guard Prods., Inc.</i> , 2022 WL 1097363 (Fed. Cir. Apr. 13, 2022)	23
<i>In re Clay</i> , 966 F.2d 656 (Fed. Cir. 1992)	22
<i>In re CSP Techs., Inc.</i> , 840 F. App’x 577 (Fed. Cir. 2021)	14
<i>In re Mouttet</i> , 686 F.3d 1322 (Fed. Cir. 2012)	24
<i>In re Preda</i> , 401 F.2d 825 (C.C.P.A. 1968)	2
<i>In re Wood</i> , 599 F.2d 1032 (C.C.P.A. 1979)	21

<i>InductEV Inc. v. Witricity Corp.</i> , IPR2021-01167, Paper 31 (Nov. 22, 2022).....	2
<i>Intel Corp. v. PACT XPP Schweiz AG</i> , 61 F.4th 1373 (Fed. Cir. 2023).....	12
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398, 417 (2007)	13, 22
<i>Microsoft v. Biscotti, Inc.</i> , 878 F.3d 1052 (Fed. Cir. 2017)	2
<i>Netflix, Inc. v. DivX, LLC</i> , 80 F.4th 1352 (Fed. Cir. 2023).....	22
<i>Winner Int’l Royalty Corp. v. Wang</i> , 202 F.3d 1340 (Fed. Cir. 2000)	22
<i>Wyers v. Master Lock Co.</i> , 616 F.3d 1231, 1238 (Fed. Cir. 2010)	13, 22

LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 11,178,116 (“116 patent”)
1002	Prosecution History of U.S. Patent No. 11,178,116
1003	Declaration of Samrat Bhattacharjee, Ph.D.
1004	Curriculum Vitae of Samrat Bhattacharjee, Ph.D.
1005	U.S. Patent Application Publication 2003/0028493 (“Tajima”)
1006	U.S. Patent Application Publication 2003/0200176A1 (“Foster”)
1007	International Application Publication WO 2004/008289A2 (“Hayhurst”)
1008	U.S. Provisional Application 60/396357 (“Hayhurst-Provisional”)
1009	Coversheet of U.S. Provisional Application 60/396357
1010	Application Data for Provisional Application 60/396357
1011	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.)
1012	Security First Innovation’s 2023-08-14 Infringement Contentions, Chart C in <i>Security First Innovations, LLC v. Google LLC</i> , 2-23-cv-00097 (E.D. Va.) (“Contentions”)
1013	U.S. Patent Application Publication 2004/0049687 (“Orsini”)
1014	International Application Publication WO 2001/22322 (“Dickinson”)
1015	U.S. Patent No. 10,452,854 (“854 patent”)
1016	U.S. Patent No. 6,021,391 (“Shyu”)
1017	U.S. Patent Application Publication 2004/0049700 (“Yoshida”)
1018	U.S. Patent Application Publication 2004/0003272A1 (“Bantz”)
1019	International Application Publication WO 2001/015162A2 (“Benaloh”)
1020	U.S. Patent Application Publication 2002/0194209 (“Bolosky”)
1021	U.S. Patent No. 6,819,766 (“Weidong”)
1022	U.S. Patent No. 4,238,853 (“Ehrsam”)

Exhibit	Description
1023	U.S. Patent No. 7,277,941 (“Ignatius”)
1024	U.S. Patent Application Publication 2005/0216754 (“Ehud”)
1025	International Application Publication WO 2004/057461A2 (“Ogihara”)
1026	U.S. Patent No. 7,178,033 (“Garcia”)
1027	U.S. Patent No. 6,490,353 (“Tan”)
1028	U.S. Patent Application Publication No. 2006/0064386 (“Marking”)
1029	U.S. Patent No. 7,529,834 (“Birrell”)
1030	U.S. Patent Application Publication 2001/0037474A1 (“Steegmans”)
1031	U.S. Patent Application Publication 2004/0172476A1 (“Chapweske”)
1032	U.S. Patent No. 7,099,994 (“Thayer”)
1033	U.S. Patent No. 6,151,659 (“Solomon”)
1034	R. L. Rivest, “ <i>All-or-nothing encryption and the package transform</i> ,” Proc. Of the 4 th Intl. Workshop on Fast Software Encryption 1997, (E. Biham, ed.), Lecture Notes in Computer Science, 1267 (1997) pp. 210–218. (“Rivest”)
1035	U.S. Patent No. 6,308,277 (“Vaeth”)
1036	U.S. Patent Application Publication 2001/0053221A1 (“Takeda”)
1037	Security First Innovation’s 2023-08-14 Infringement Contentions, Chart D in Security First Innovations, LLC v. Google LLC, 2-23-cv-00097 (E.D. Va.)
1038	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)
1039	U.S. Patent Application Publication 2018/0367509A1 (“116 Publication”)
1040	ABS: The Apportioned Backup System (“Cooley”) https://pdos.csail.mit.edu/archive/6.824-2004/reports/cooley.pdf
1041	U.S. Patent Application Publication 2003/0081790A1 (“Kallahalla”)
1042	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)

Exhibit	Description
1043	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)
1044	U.S. Patent No. 9,338,140 (“140 patent”)
1045	Supplemental Declaration of Samrat Bhattacharjee, Ph.D. [SUPPLMENTAL EVIDENCE – NOT FILED]
1046	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.) [SUPPLMENTAL EVIDENCE – NOT FILED]
1047	Declaration of Rachel J. Watters Relating to Exhibit 1034 [SUPPLMENTAL EVIDENCE – NOT FILED]
1048	RESERVED
1049	RESERVED
1050	RESERVED
1051	RESERVED
1052	RESERVED
1053	RESERVED
1054	RESERVED
1055	RESERVED
1056	RESERVED
1057	RESERVED
1058	RESERVED
1059	RESERVED
1060	RESERVED
1061	RESERVED
1062	RESERVED
1063	RESERVED

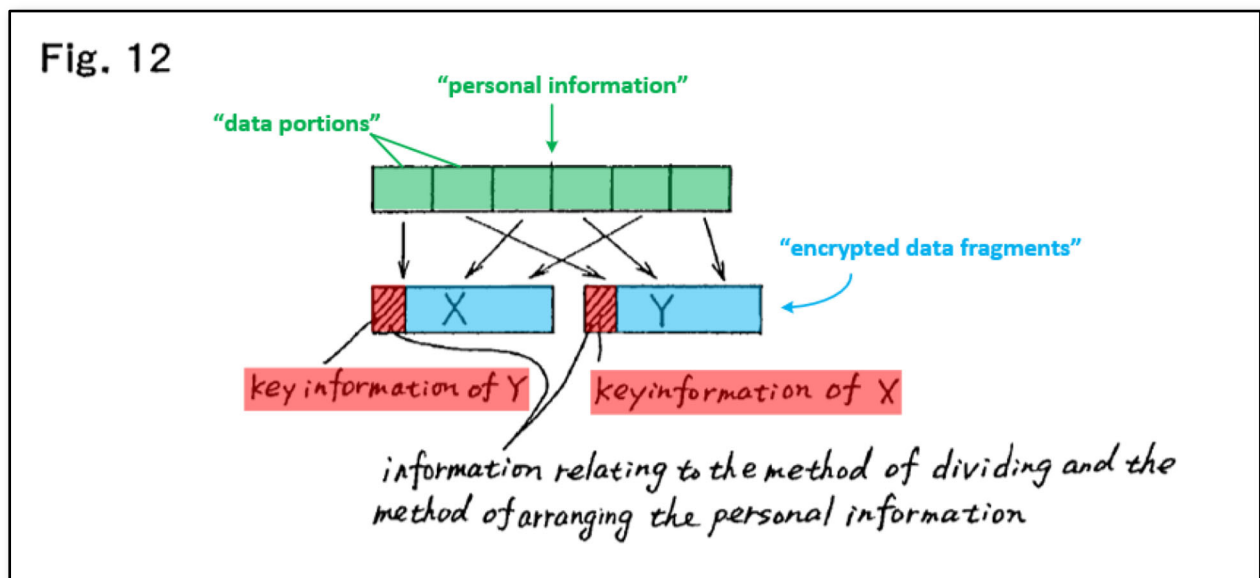
Exhibit	Description
1064	RESERVED
1065	RESERVED
1066	RESERVED
1067	RESERVED
1068	RESERVED
1069	RESERVED
1070	RESERVED
1071	RESERVED
1072	U.S. Patent Application Publication No. 2004/0019900
1073	U.S. Patent Application Publication No. 2002/0083438
1074	U.S. Patent No. 7,076,661
1075	U.S. Patent No. 6,771,657
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

Exhibit	Description
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
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.
1112	U.S. Patent Application Publication No. 2004/0010699
1113	European Patent Application Publication No. EP1,564,686

Exhibit	Description
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 1: TAJIMA

For Ground 1, SFI's arguments concern only limitation [1D]: *"storing each data chunk [Tajima's data fragments]...together with one of the plurality of obfuscated different encryption keys."* SFI argues Tajima's "key information" attached to each data fragment (red below) does not include, and POSAs had no obvious reason to include, the encryption key.



A. Tajima's Key Information Includes the Key

Petitioner explained that POSAs understood that Tajima's "key information" includes the key because:

- (1) Tajima says "key information" (and identifies nothing else) is "used to decrypt" data fragments (Tajima, [0112], [0114]), decryption requires the key, and Tajima never describes obtaining keys from elsewhere (Petition, 20-21 (citing Bhattacharjee, ¶¶97-98, 103)); and

(2) Tajima’s embodiments describe a technique of dividing “key information” into data portions (Tajima, [0109]-[0110], [0113]-[0114]), and Tajima’s claims to that technique recite dividing “the encryption key” into data portions (Petition, 21-22 (citing Bhattacharjee, ¶¶99-102)).

SFI’s contrary arguments fail.

1. Petitioner Did Not Rely On Inherency

An argument based on what POSAs “understood from [Tajima]’s teachings” is “***not*** [an] inherency”¹ argument (*InductEV Inc. v. Witricity Corp.*, IPR2021-01167, Paper 31, 45 (Nov. 22, 2022)) as SFI erroneously alleges. POR, 3.

A reference discloses a limitation by the “specific teachings of the reference [and] the inferences which [a POSA] would reasonably draw therefrom.” *In re Preda*, 401 F.2d 825, 826 (C.C.P.A. 1968); *see also ArthroCare Corp. v. Smith & Nephew, Inc.*, 406 F.3d 1365, 1373-74 (Fed. Cir. 2005) (“even if a piece of prior art does not expressly disclose a limitation, it anticipates if a [POSA] would understand the prior art to disclose the limitation and could combine the prior art description with his own knowledge to make the claimed invention”); *see also Microsoft v. Biscotti* at 1065, 1068 (cited POR, 3).

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

2. POSAs Understood Tajima’s Key Information Includes the Key

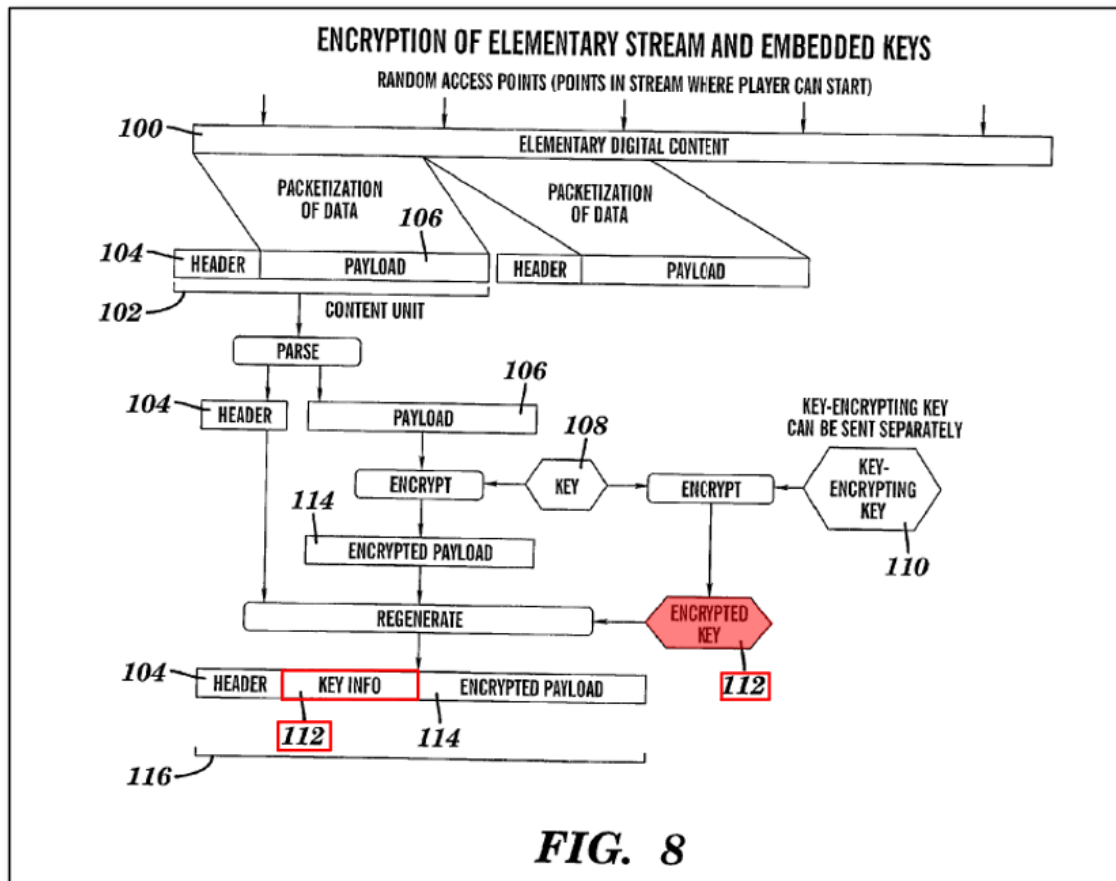
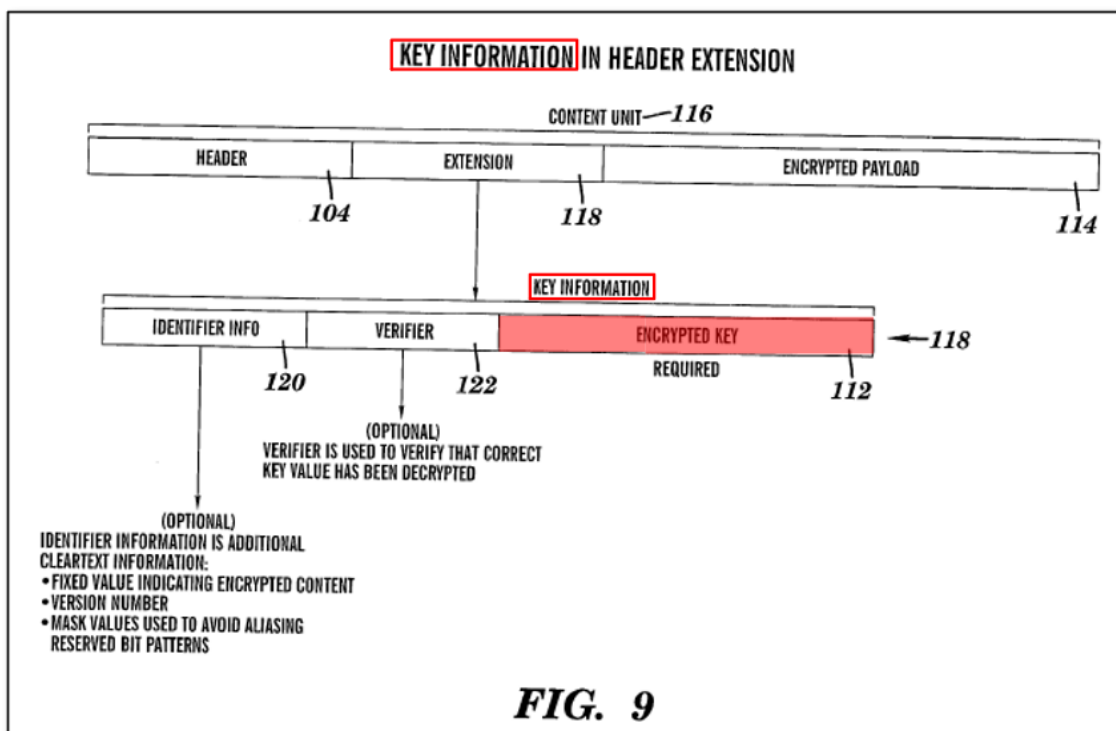
Petitioner did not “acknowledge[] that ‘Tajima never says...anything’ *about what constitutes information regarding the key*” as SFI disingenuously alleges. POR, 4 (misquoting Petition, 20). Petitioner explained “Tajima never says that anything else beyond the key information is needed for decrypting” and “does not disclose any additional steps nor any separate key management infrastructure,” which informs POSAs that the keys required for decryption are included in the key information. Petition, 20.

SFI alleges in conclusory fashion that it “does not logically follow” from Tajima’s silence about “additional steps nor any separate key management infrastructure” that Tajima’s key information includes the key (POR, 4) but identifies no flaw in Petitioner’s logic. Instead, SFI only knocks down an inherency strawman argument that Petitioner never made. *See* POR, 4-5 (“[i]f the information regarding the key indicates...information that can be used to derive the key, such information could be ‘used to decrypt’ a data fragment without being the key itself”). Proposing alternative *undisclosed* ways Tajima could hypothetically decrypt data fragments using key information fails to rebut Petitioner’s straightforward explanation that POSAs understood that Tajima’s key information includes the key. Bhattacharjee-Reply, ¶¶15-17.

3. SFI's Allegations About What Key Information Means Fail

SFI argues if Tajima meant to say the “key,” it would not need the terms “key information” or “information regarding the key.” POR, 3. But SFI ignores Dr. Bhattacharjee’s explanation that POSAs “understood that Tajima’s key information may (and likely would) include *additional* metadata about the key to facilitate [data] recover[y],” which explains that “key information” is a genus of information that includes the “key” and related information added to facilitate data recovery. Bhattacharjee, ¶103 (cited Petition, 21); Bhattacharjee-Reply, ¶¶5-6.

That opinion is corroborated by other prior-art references that used “key information” in the same way. Bhattacharjee, ¶131. For example, Foster encrypts segments of data with respective “title key[s]” and attaches to each encrypted data segment its “encrypted title key 112.” Foster, [0064]-[0067]. As shown in Foster’s Figures 8-9 (annotated below), Foster calls the information that includes the “encrypted key 112” and additional data the “*key information*,” corroborating a POSA’s understanding that “key information” encompasses information that includes the key and other types of information. Bhattacharjee-Reply, ¶¶7-8.

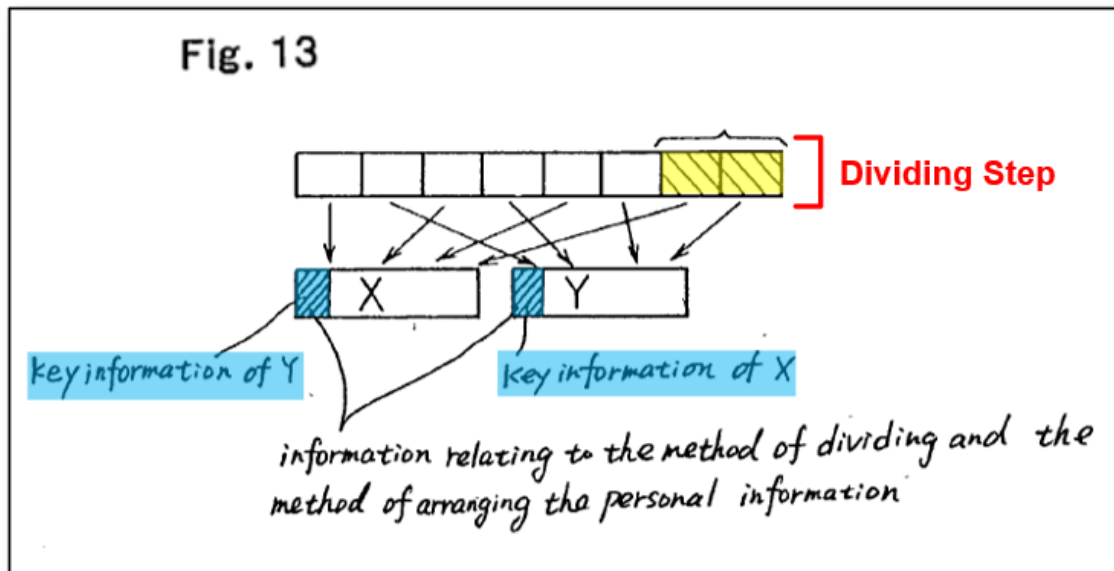


SFI's '854 patent likewise corroborates that “key information” encompasses the key. It says “[t]he workgroup key concept allows for enhanced protection of information assets by encrypting key information stored within the shares” (EX1015 79:66-80:4), and says “[w]hen a workgroup key is utilized to protect the encryption key,” the “encryption key [is] encrypted with the workgroup key prior to being stored within the shares” (EX1015, 80:24-28). SFI's own patent uses “key information” to refer to an encryption key. Bhattacharjee-Reply, ¶¶9-14 (citing EX1113, [0090]-[0098]; EX1114, [0022] as further corroboration).

4. SFI Does Not Dispute That Tajima's Claims Disclose That “Key Information” Includes the Key

Multiple Tajima claims recite “divid[ing] the encrypted personal information and *the encryption key* used in the encryption into a plurality of data portions.” Petition, 21-22. As the Petition explained, the claimed dividing step is performed on the “key information” in the FIG. 13 embodiment shown in Tajima's FIG. 13 (annotated below). Tajima, [0113]-[0114]. This demonstrates that the “key information” (highlighted yellow) divided into data portions in this step includes “the encryption key” as claimed. As the Petition further explained, POSAs understood that when Tajima uses the same term “key information” to describe the information attached to the data fragments (highlighted blue in FIG. 13), Tajima means the same thing—i.e., information that includes the encryption key. Petition,

21-22 (citing Bhattacharjee, ¶¶99-102); Bhattacharjee-Reply, ¶¶18-23. SFI does not dispute *any* of this and Dr. Rubin provided no opinion at all.



Instead, SFI ignores the FIG. 13 embodiment and alleges that Tajima’s Figure 11 embodiment “ha[s] no bearing” on Ground 1, which relies on “the Figure 12 and 13 embodiments.” POR, 5. But, the Petition “relied” on the FIG. 11 embodiment only to corroborate what the FIG. 13 embodiment also discloses—performing the dividing step on the “key information” that Tajima’s claims make clear is performed on the “encryption key” itself. Bhattacharjee, ¶¶99-102. The Petition did ***not*** combine “distinct teachings” in Tajima (POR, 5), but instead showed that the claims confirm that Tajima uses the term “key information” to mean information that includes the key. That showing is un rebutted. Bhattacharjee-Reply, ¶¶19-23.

B. Including Tajima’s Key in Tajima’s Key Information Was Also Obvious

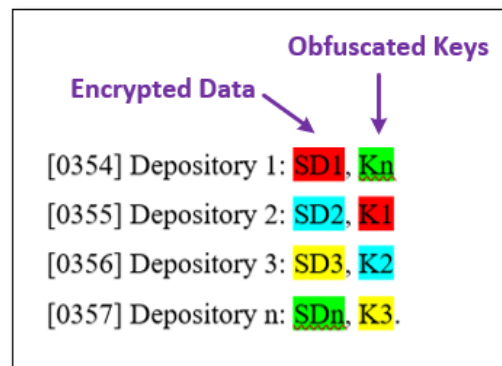
Petitioner also explained that including the keys in Tajima’s “key information” was “an obvious and conventional way *to implement what Tajima discloses*—i.e., a system that needs only the key information to decrypt data fragments and not additional key management infrastructure.” Petition, 22.

SFI alleges that “no evidence or explanation” supports Petitioner’s assertion, which is false. POR, 5-6. The Petition’s obvious implementation relies on the same evidence in Tajima’s disclosure that (1) nothing more than the key information attached to the data fragment is used to decrypt them, (2) all the information needed to recover the personal information is stored in the data fragments, and (3) Tajima’s claims demonstrate the “key information” includes the key. Petition, 21-22 (citing Bhattacharjee, ¶¶96-106); Bhattacharjee-Reply, ¶¶24-25.

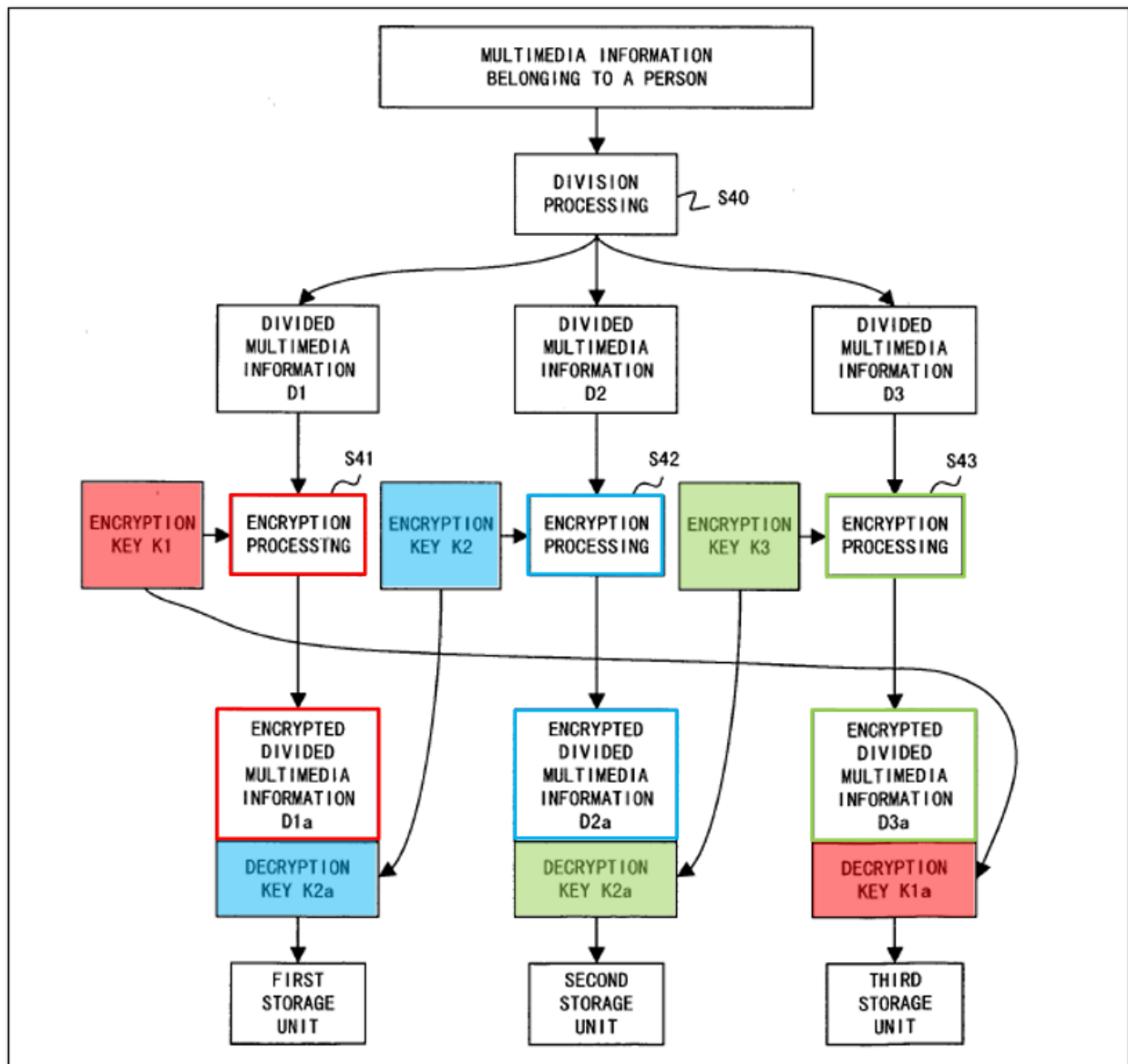
Thus, even if that evidence were found not to demonstrate that Tajima’s key information includes the key, straightforwardly implementing Tajima that way plainly would have been obvious and desirable so that a site authorized to recover Tajima’s secured data “need only retrieve the stored encrypted data fragments to acquire the keys needed to decrypt them,” rather than requiring “a separate key-management system” to store those keys. Bhattacharjee, ¶104; EX1099 (“Rubin-Depo.”), 177-178 (admitting keys “ha[ve] to be stored somewhere”). SFI never

disputes that implementing Tajima in this way would have been obvious and beneficial. Bhattacharjee-Reply, ¶¶26-27.

SFI *also* does not dispute this implementation was conventional. Storing an encryption key with the encrypted data was known. Like Tajima, EX1013 and EX1113 both store encryption keys with encrypted data it cannot decrypt. EX1013, [0294]-[0299], [0354]-[0357] (reproduced below); EX1113, [0090]-[0098], FIG. 13 (annotated below); Bhattacharjee, ¶¶31-32, 54 (cited Petition, 6); Bhattacharjee-Reply, ¶¶28-32.



EX1013, [0354]-[0357] (Annotated)



EX1113, FIG. 13 (Annotated)

POSAs knew that to implement Tajima, either keys are included in the key information stored with the data, or keys are stored and maintained elsewhere. Both techniques were known, “conventional,” and obvious. Bhattacharjee-Reply, ¶¶28-32; Rubin-Depo., 177-178. Unable to dispute this, SFI alleges that “to the extent” Petitioner relies on “common sense,” that reliance would be improper. POR, 6

(citing *DSS Tech.*). Unlike in *DSS Tech.*, where the Federal Circuit faulted the Board’s invocation of “ordinary creativity” as a “wholesale substitute for reasoned analysis and evidentiary support” (*DSS Tech.* at 1376-77), Dr. Bhattacharjee and the Petition straightforwardly reasoned that implementing Tajima so that nothing beyond the key information is needed to decrypt the data fragments (as Tajima discloses), rather than implementing key-management technology (about which Tajima says nothing), would have been conventional and obvious. Petition, 20-22; Bhattacharjee, ¶¶96-104.

Because the Petition did not “invoke[] common sense to fill in a *missing* limitation” (*DSS Tech.* at 1374, emphasis original), but instead relied on reasoned analysis that SFI ignores, the Board need not find “the limitation in question [to be] unusually simple and the technology particularly straightforward” (*id.* at 1374).

C. SFI’s Lack-of-Motivation Argument Fails

SFI alleges that the Petition failed to demonstrate motivation and points to Petitioner’s acknowledgement that storing plaintext keys has risks. POR, 6-7. But SFI ignores that Tajima addresses some of that risk by storing key information with a data fragment it cannot decrypt. Petition, 33; Bhattacharjee, ¶140. The fact that POSAs knew that storing plaintext keys with encrypted data, even when obfuscated, still has risk does not make that known implementation non-obvious. Bhattacharjee-

Reply, ¶¶32. Obviousness does not require the “most desirable” implementation.” *In re Fulton*, 391 F.3d 1195, 1200 (Fed. Cir. 2004).

Including keys in Tajima’s key information meant the authorized service site “need only retrieve the stored encrypted data fragments to acquire the keys needed to decrypt them, [] rather than implementing a separate keystore or key management system” to store them (Bhattacharjee, ¶104), while Tajima’s obfuscation protects against attackers that acquire some but not all encrypted data fragments. Bhattacharjee, ¶141; Bhattacharjee-Reply, ¶33. This beneficial implementation is not rendered non-obvious by other obvious modifications that could improve Tajima’s security. *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1379-81 (Fed. Cir. 2023)

II. GROUND 2: TAJIMA-FOSTER

Ground 2 applies “Foster’s key-encryption technique to encrypt Tajima’s key[s]...to benefit from the increased level of security” of storing encrypted rather than plaintext keys. Petition, 37. As the Board recognized at institution, that motivation existed because POSAs knew key encryption keys (“KEKs”) “provided even further security” in systems (like Tajima’s) that store encrypted data portions paired with unencrypted key information. DI, 17. SFI provides no reason for the Board to find differently now.

A. Even if Tajima’s and Foster’s Fields/Problems Were Different, Their Combination Was Still Obvious

SFI argues POSAs would not have combined Tajima and Foster because they are allegedly “directed to entirely different fields and to different problems.” POR, 9-10. First, Tajima and Foster are not in “entirely different fields.” POR, 9. Tajima and Foster are both in the same field as the ’116 patent: “securing data from unauthorized access or use” (POR, 40). *See, e.g.*, Foster, [0003] (relates to “security of content [data]”); Tajima, [0044] (“improve[s] the security of personal information [data]”); Bhattacharjee-Reply, ¶¶34-35.

But even were that not the case, SFI cites no authority limiting obvious combinations to references in the same field and/or addressing the same problem. Instead, “familiar items may have obvious uses beyond their primary purposes.” *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1238 (Fed. Cir. 2010). Thus, even if Tajima’s and Foster’s fields and problems were different, POSAs had reason to modify Tajima to apply Foster’s teaching to use a KEK to encrypt keys to achieve the well-known benefits of securing Tajima’s encryption keys. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (“design incentives...can prompt variations...in the same field *or a different one*”). Bhattacharjee-Reply, ¶36.

B. It Would Have Been Obvious to Encrypt Tajima’s Encryption Keys Using the Known KEK-technique and Store the Encrypted Keys With Data Fragments

The Petition demonstrated, supported by expert testimony *and corroborating evidence*, that POSAs had reason to “us[e] Foster’s key-encryption technique to encrypt Tajima’s keys before attaching them to different encrypted fragments” (Petition, 37) so that even an attacker who obtained all data fragments would not acquire all of Tajima’s keys in plaintext form. Petition, 34-37 (citing Bhattacharjee, ¶¶141-154); DI, 18-19. SFI’s challenges to Petitioner’s motivation-to-combine all fail.

1. Tajima’s and Foster’s Alleged “Lack of Critical Disclosures” Do Not “Preclude Their Combination”

SFI argues POSAs would not have been motivated to combine Tajima and Foster because (1) Tajima allegedly “does not disclose attaching the key itself to a data fragment” and (2) Foster’s “content units” are allegedly neither the claimed *data chunks* nor “correspond to Tajima’s data fragments.” POR, 18-19. SFI’s arguments fail because they improperly attack the references individually, rather than address Petitioner’s *combination*. *In re CSP Techs., Inc.*, 840 F. App’x 577, 585 (Fed. Cir. 2021) (obviousness “cannot be overcome by attacking references individually” when unpatentability “is based upon the...combination”).

SFI’s argument (1) above fails if the Board agrees that Tajima’s “key information” includes Tajima’s keys as discussed *supra* §I.A. But even if the Board

disagrees, SFI's argument still fails because the Tajima-Foster combination uses "*Foster's key-encryption* technique to encrypt *Tajima's keys* before *attaching them* to different encrypted fragments" (Petition, 37), which the Board recognized at institution. DI, 18-19 ("Foster's key-encryption technique...involves transmitting and storing the encrypted key itself"); *see also* Petition, 38-42 (Tajima-Foster *combination* stores encrypted keys with the data); Bhattacharjee-Reply, ¶¶37-38.

SFI's argument (2) above fails because the claimed *data chunks* are met in Tajima-Foster by *Tajima's data fragments* (not Foster's packets), which SFI does not dispute are *data chunks*. Petition, 37-38, 40-41. Allegedly "significant" differences between Foster's packets and *data chunks* (POR, 20-23) are irrelevant in Tajima-Foster. SFI never explains how any alleged differences between Foster's "packet payloads," Tajima's data fragments, and the claimed *data chunks* (POR, 20-21) would have dissuaded POSAs from using Foster's well-known KEK technique to encrypt Tajima's encryption keys. Those alleged distinctions are irrelevant because POSAs knew the enhanced security provided by a KEK is not dependent on the content of data being secured. Moreover, Foster's KEK encrypts *encryption keys*, not any data SFI alleges have "significant" differences. Bhattacharjee-Reply, ¶39; Rubin-Depo., 22-25, 154-156.

2. Encrypting Tajima's Keys Would Have Further Secured Tajima's Data

SFI's argues that using Foster's KEK in Tajima would be "redundant" because Tajima's key information "is already secured" by "attaching it to a data fragment it cannot decrypt" and "storing different data fragment/key information combinations in different locations" (POR, 23). SFI's argument ignores Tajima's vulnerability that Foster's key-encryption addresses.

As Petitioner explained, "an attacker [] able to recover all of Tajima's data fragments...will possess all of the plaintext keys used to encrypt the entire data set." Petition, 33. Decrypting the data fragments would simply require determining the correct encryption key/data fragment combinations, which an attacker could easily do. Petition, 33-34; Rubin-Depo., 22-23, 153-154. SFI does not dispute this.

By using "Foster's key-encryption technique to encrypt Tajima's keys before attaching them to different encrypted fragments" (Petition, 37), an attacker that successfully acquired all data fragments would possess only undecipherable encrypted (rather than plaintext) keys. Petition, 34-35. SFI never disputes that Tajima-Foster increases security in this way. Requiring an attacker to obtain KEKs to decrypt Tajima's encryption keys *in addition to* de-obfuscating them is not "redundant" to only having to de-obfuscate them. Bhattacharjee-Reply, ¶¶41-44.

SFI's redundancy argument (POR, 24 citing EX2033, ¶75) never refutes that applying Foster's key-encryption to Tajima's keys provided more security.

Bhattacharjee-Reply, ¶44; EX1090, 2:39-41 (“The more difficult it is for an unauthorized entity to obtain a valid key, the more secure the cryptographic scheme.”); Rubin-Depo., 154-156 (confirming that security should be put “in the keys and not in the hiding of your algorithms”). That Tajima did not suggest that its security is inadequate (POR, 24) does not make using Foster’s known KEK-technique non-obvious. *Cole Kepro Int’l, LLC v. VSR Indus., Inc.*, 695 F. App’x 566, 570 (Fed. Cir. 2017) (that a prior art reference discloses a solution to a problem “does not discourage,” by that fact alone, seeking improvements to that solution).

3. Foster Supports, Rather Than Discourages, Tajima-Foster

SFI alleges that Tajima-Foster “eliminat[es] the benefits of both systems” and “cannot achieve the objective of either.” POR, 25. Not so.

SFI argues that Tajima pairs key information with a data fragment that the key information did not encrypt, whereas it is “essential” in Foster to support synchronization by keeping each encrypted key with the portion of content the key encrypted. POR, 25-26. That distinction is irrelevant because Tajima-Foster does not modify Foster or use Foster’s data. Instead, Tajima-Foster modifies ***Tajima*** to secure ***Tajima’s data***, which does not require synchronization because (unlike Foster) Tajima-Foster is not concerned with synchronizing media data. Petition, 37-39. The benefits of using Foster’s KEK in Tajima is independent of Foster’s synchronization. Synchronization of Foster’s data is irrelevant to Tajima-Foster because Tajima-

Foster does not restore Foster's data. Bhattacharjee-Reply, ¶¶45-46; *Ex Parte Richard Kane*, APPEAL 2016-005068, 2018 WL 2332503, at *9 (May 14, 2018) (alleged changes to "basic principles" of the secondary reference were irrelevant because "it is the primary reference...which is being modified in view of" the secondary reference).

Contrary to SFI (POR, 25-26), encrypting Tajima's key with a KEK does not eliminate Tajima's benefits or objectives. Instead, Tajima-Foster *improves Tajima's* security, furthering Tajima's objective of preventing unauthorized access to personal information. Tajima, [0026], [0042]-[0043]. That Tajima-Foster improves security of Tajima's data fragments should an attacker successfully acquire all of them is undisputed. Bhattacharjee-Reply, ¶47.

SFI's "teaching away" caselaw is inapposite. POR, 27 (quoting *DePuy Spine* and *AstraZeneca*). Foster keeps encrypted media segments with their keys to facilitate random access to Foster's media content. Foster, [0006]-[0007]. That does not "discourage" using Foster's KEK (a well-known technique) with Tajima's obfuscation technique (which stores a key separate from the data it secures) because *Tajima's data fragments* are not randomly accessed nor would there have been a need to do so. Petition, 33-37; Bhattacharjee-Reply, ¶47.

4. Petitioner Demonstrated a Reasonable Expectation of Success in Implementing Tajima-Foster

Petitioner demonstrated that POSAs reasonably expected success in straightforwardly using Foster's key-encryption technique to encrypt Tajima's keys before attaching them to different encrypted fragments. SFI does not dispute this was well within POSAs' skill. Petition, 39-40 (citing Bhattacharjee, ¶¶160-163, 167); Bhattacharjee-Reply, ¶40. The Petition need not have demonstrated reasonable expectation of success in combining Tajima and Foster in other ways. POR, 22-23.

III. GROUND 3: TAJIMA-RIVEST

SFI's lack-of-motivation arguments for the Tajima-Rivest combination fail. POR, 28-31. Bhattacharjee-Reply, ¶¶48-51.

SFI argues that performing AoNT using Tajima's public key would not add security because anyone knowing the user's public key could invert the transformation. POR, 29-30. That argument fails because inverting Tajima's transformed data would also require knowing (1) that AoNT was applied in the first place and (2) that a user's public key, and which user's public key, was used in the transformation—none of which is known by an attacker or apparent from the data fragment itself. Bhattacharjee-Reply, ¶¶48-50.

SFI argues POSAs would not have applied AoNT because Rivest says “all-or-nothing encryption has terrible error propagation properties.” Rivest, 216; POR, 31. Rivest is clearly not discouraging the use of its own transform. Rivest explains

that reliable transmission/error correction should be used to address this problem. Moreover, Tajima-Rivest avoids (hypothetical) error propagation because individual transformed message blocks are kept and transmitted together in Tajima-Rivest's transformed data. Bhattacharjee-Reply, ¶51.

IV. GROUND 4: TAJIMA-RIVEST-SHYU

SFI's lack-of-motivation arguments for the Tajima-Rivest-Shyu combination fail. POR, 32-34.

SFI argues that Shyu's application of different encryption algorithms to different pieces of the same dataset violates "Kerckhoffs' Principle." POR, 32-34. That is incorrect and irrelevant. "Kerckhoffs' Principle" states a preference for relying on secret keys rather than relying on keeping "the encryption scheme itself" a secret (i.e., keeping secret *how* the algorithm *itself* works). EX2007, 17-18; Bhattacharjee-Reply, ¶¶52-53.

Shyu does not use secret algorithms. Shyu selects from among *known* algorithms to secure different data segments, thereby keeping some data segments secured even if another segment has been deciphered by an attacker. Shyu, 1:24-42; 3:12-38, 3:56-60 (cited Petition, 48-49). Withholding what known algorithms were used is not the secret Kerckhoffs' Principle refers to. Bhattacharjee-Reply, ¶54. Moreover, Kerckhoffs' Principle does *not* say that secret algorithms provide *no* security. *Id.*; EX2007, 18; Rubin-Depo., 155-156.

Finally, SFI argues that because Shyu’s technique secures data during transmission “from a single source to a single destination” it would not benefit Tajima’s system, which transmits data fragments to “different destinations.” POR, 34-45. That argument fails because the Tajima-Rivest-Shyu **combination** applies Shyu’s principle to increase security of Tajima’s data fragments after **storing**, not during transmission. Bhattacharjee-Reply, ¶55.

V. GROUND 5: FOSTER-HAYHURST

A. Hayhurst is Analogous Art

1. Hayhurst Has the Same Field of Endeavor.

SFI argues “the ’116’s field is securing data,” including securely storing and communicating data. POR, 39-40. Hayhurst is in the same field.

Hayhurst’s “**Technical Field**” is “electronic media delivery...including the **secure handling and storage** of such media.” Hayhurst, [0002]; DI, 10. That should be dispositive that Hayhurst is analogous. *In re Wood*, 599 F.2d 1032, 1036 (C.C.P.A. 1979). Hayhurst’s specification reinforces this. Hayhurst, [0021] (“provid[ing] increased **security** from piracy”), [0007] (“**encrypt[ing]**” “**segments**” further “prevent[s] unauthorized viewing”); Bhattacharjee-Reply, ¶¶60-68.

Hayhurst’s field is not limited to “decentralized media delivery” (POR, 41)—that is **how** Hayhurst provides “**security**” of stored data. Hayhurst, [0008]. Like Hayhurst, the ’116 patent **itself** says it secures data via “geographical separation of...storage facilities.” EX1001, 20:28-38. Bhattacharjee-Reply, ¶69.

SFI argues Hayhurst does not teach that security was a problem “or that its invention addresses a need for more security.” POR, 42-43. 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). Moreover, Hayhurst’s “approach” “provides increased security.” Hayhurst, [0021]. Thus, Hayhurst recognized a need for “increased security” and addressed that need. Bhattacharjee-Reply, ¶¶69-80; Rubin-Depo., 108-109.

SFI cites two pre-*KSR* 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 because they involved significant technical distinctions that are absent here. As discussed, the ’116 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 uses a technique the ’116 patent itself says secures data (distributed data storage). Bhattacharjee-Reply, ¶¶65-80.

2. Hayhurst is Reasonably Pertinent to a ’116-Identified Problem.

The ’116 patent identifies several problems that Hayhurst is reasonably pertinent to.

User-Independent Security. SFI only addresses the '116 patent's alleged problem of providing a “cryptographic system whose security is user independent.” POR, 44. Hayhurst is reasonably pertinent to that problem and addresses it by segmenting and distributing data without requiring user action. Hayhurst, [0027]. As the Board correctly observed in a related matter, users cannot undermine Hayhurst's security because “no one subscriber unit has more than one media segment, and a single segment has little value.” IPR2024-00215, Paper 15, 22; Hayhurst, [0021], [0029]; Bhattacharjee-Reply, ¶¶82-90. Rubin-Depo., 115-120, 125-130.

Computer-Network Security. Hayhurst is also reasonably pertinent to other problems the '116 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, 1:26-33; 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[ri]ng [] piracy” ([0008]). Bhattacharjee-Reply, ¶¶91-93.

Distributed Storage. The '116 patent splits and stores data “in geographically remote secure data storage facilities.” EX1001, 5:18-22. It does that to address alleged problems with “protecting...against composition of any individual data

storage facility” (5:18-22) and data “remain[ing] whole and intact and subject to attack” (57:10-24). Hayhurst’s distributed storage device addresses those problems and solves them in the same way. Rubin-Depo., 124-135; Bhattacharjee-Reply, ¶¶94-101.

B. POSAs Had Motivation For Foster-Hayhurst

Petitioner established that POSAs had reason to implement Foster’s system using Hayhurst’s distributed-storage technique because it would, for example, reduce a content provider’s bandwidth requirements and increase Foster’s security by storing data portions in different storage devices. Petition, 61-64.

SFI argues Hayhurst is incompatible with Foster’s goal of “avoiding delays” for “streaming live television.” POR, 47-48. 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 encrypting content *stored* for and by recipient(s) (e.g., video-on-demand). Foster, [0064]; Bhattacharjee-Reply, ¶¶102-111. In (at least) Foster’s storage context—relied upon in the Petition (51-53)—POSAs would have recognized the benefits of Foster-Hayhurst.

1. Foster Stores Encrypted Content.

Foster teaches that placing an encryption key with encrypted data (to support “synchronization”) may reduce (i) the risk of applying the wrong key to an encrypted chunk of data and (ii) the time it takes to locate the correct key for decrypting a chunk of data. Petition, 52-53 (citing Foster, [0004]-[0007]). Foster, [0002]-[0007].

SFI argues Foster’s “fundamental goal” is to use “synchronization” to “reduc[e] delays in viewer access to content *as it is transmitted*” in real-time. POR, 48-49 (citing Foster, [0008]). But that same sentence in Foster that SFI cites *also* teaches attaching a key to encrypted data “for synchronized...*storage*.” Foster, [0008]. Foster repeatedly says synchronization is useful for either data “transmission...*or storage*.” Foster, Abstract; *see also* [0007]-[0008], [0048], [0064], [0079], claim 11; Bhattacharjee-Reply, ¶¶112-116. The Board recognized this at institution. DI, 21-22 (Foster “synchronously *store[s]* the encrypted content”). SFI *admitted* in IPR2024-00214 (Paper 22, 44, 51) that Foster “*teaches*...the ‘recipient 430 can....*store* the encrypted content.’” *See also* Rubin-Depo., 187-191, EX2033, ¶148. That Foster stores its encrypted data should not be genuinely disputed.

Foster is explicit 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 along [with] all information necessary to decrypt the content.”); Bhattacharjee-Reply, ¶117; 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 at a] personal computer” for on-demand access (i.e., when the user wants to view stored content after downloading/storing). Foster, [0005], [0049] (storing “content on media server”);

FIG. 1 (content is “stream[ed] *or stored*”); Bhattacharjee-Reply, ¶¶118-120; EX2039, 6-10 (DRMS “safeguards content when *at rest* [i.e., stored],” including when “*stored* on a receiving device”).

Consistent with its DRMS disclosures, Foster teaches processing datasets for the MPEG-standard’s “program stream,” which Foster says is intended for use “*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], [0042]-[0043]; Bhattacharjee-Reply, ¶¶121-127; Rubin-Depo., 82-83. Foster’s text makes clear that Foster’s teachings include storage-based embodiments.

Finally, Foster’s streaming in a conditional access system (“CAS”) is not limited to streaming “live” broadcasts. POSAs knew CAS is used in video-on-demand (VOD) systems, where “content *is stored pre-encrypted* on hard drives in the VOD server” (EX1110, [0007]) and stored in “*storage* media” (EX1072, [0043]); Bhattacharjee-Reply, ¶¶128-142 (citing also EX1073, [0001]-[0004], [0043]; EX1097, 2:32-52; EX1075, 1:51-67; EX1076, 9:53-10:5; EX1077, 1:48-65, 3:56-5:8). Rubin-Depo., 85-94.

2. Foster-Hayhurst Is Consistent With Foster’s Goals.

Relying on its narrow interpretation of Foster as being limited to live streaming 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, 56-68. These critiques lack merit.

SFI’s first two critiques depend on narrowly interpreting Foster as being concerned **only** with real-time video streaming. POR, 61-64 (“Foster seeks to securely stream content, *e.g.*, live television, without delay....”). But as discussed above (§V.B.1), Foster is not so limited and also concerns **storing** secured data. Foster, [0007]-[0008]. *Supra* §V.B.1; Bhattacharjee-Reply, ¶¶143-145.

SFI speculates Foster-Hayhurst would have excessive delays when a movie file is distributed amongst “thousands” of recipients. POR, 58-60. But Hayhurst’s distributed system **reduces** delay by increasing aggregate speed and efficiency of content storage/delivery by having multiple devices store and deliver content. Hayhurst, [0005], [0008]-[0009] (cited Petition, 62); Bhattacharjee, ¶¶241-243; Bhattacharjee-Reply, ¶¶145-158; EX1001, 70:10-12; Rubin-Depo., 89-93.

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

SFI cites Foster, [0053]-[0054] but that only says a key “**can** be re-encrypted with a different” KEK. Contrary to SFI’s arguments (POR, 58-60), 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, ¶¶159-162.

Moreover, POSAs knew changing a KEK in Foster-Hayhurst would be comparable to doing so in Foster because both would involve changing the KEK used for multiple segments. Bhattacharjee-Reply, ¶163. Independently, POSAs also knew how to change/replace KEKs across many devices/users. Bhattacharjee-Reply, ¶¶164-168 (citing EX1078, 4:5-28; EX1079, 544-546; EX1080, 6-7).

Regardless, Foster-Hayhurst does not distribute the KEK to user devices. Rather, as in Foster alone, Foster-Hayhurst would only give access to a KEK once authorized to decrypt the content. Foster, [0049], [0052]. Based on Hayhurst, 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, 57-58), [0021]; Bhattacharjee, ¶251 (cited Petition, 66); Bhattacharjee-Reply, ¶¶169-170.

Thus, Foster-Hayhurst does not diminish Foster’s security. *Contra* POR, 64-68. Rather, using Hayhurst’s distributed storage in Foster “provides a *high level of security*.” Hayhurst, [0008]. Hayhurst reduces unauthorized access in Foster because an attacker must collect multiple chunks from multiple storage devices, rather than from one storage device. Petition, 57-58 (citing Hayhurst, [0005], [0008]); Bhattacharjee-Reply, ¶¶171-173; Rubin-Depo., 125-130.

But even if Foster-Hayhurst were less secure than Foster in ways SFI alleges (it is not), Foster-Hayhurst added a security technique that Foster lacks (distributed storage) *and* provided the other (undisputed) benefits (e.g., speed, intelligence, efficiency, and redundancy) that also motivated Foster-Hayhurst. Petition, 62-63 (citing EX1028-EX1031); Bhattacharjee-Reply, ¶¶174-176 (citing corroboration); *Corephotonics*, 2021 WL 4944471, at *6 (“design decisions entail making tradeoffs among multiple objectives”).

SFI argues Foster “has no need for redundancy” or “efficiency/intelligence” that Foster-Hayhurst provided. POR, 67-68. But, compared to Foster’s single source, Foster-Hayhurst’s redundancy addressed known problems (e.g., power/network failure at one source) and efficiency/intelligence allowed for selecting better source(s). Bhattacharjee, ¶¶241-244; Rubin-Depo., 89-92, 135-137. Bhattacharjee-Reply, ¶¶177-182.

C. Foster’s Payloads Are “*Data Chunks*”

Claims 1/9 require “*distributing [a] data set into a plurality of data chunks*” and encrypting *data chunks*. Petitioner mapped the claimed “*data chunks*” to Foster’s “payloads” and the claimed “*data set*” to Foster’s “content.” Petition, 68-69. Each Foster payload is a portion of Foster’s content and thus “*none of* [Foster’s payloads] *are, by themselves, sufficient to reconstruct* [Foster’s content].” Petition, 69-70, 17. Nothing more is required. Bhattacharjee-Reply, ¶183.

SFI does not dispute that Foster’s payloads are individually insufficient to reconstruct Foster’s content. Instead, SFI argues Foster does not generate the claimed *data chunks* for other reasons allegedly “explained earlier.” POR, 68 (citing Section III.A.2.a.i). In that section (for Ground 2), SFI argues that: (1) “partitioning the data set into chunks increases security because when ‘data...remains whole and intact,’ it is ‘subject to attack,’” which the ’116 patent allegedly addresses “in part, by ‘performing a cryptographic parsing and splitting of the encrypted file;’” (internal quotes to EX1001, 57:10-24); and (2) Foster’s payloads are allegedly “not created to protect the data.” POR, 21-22; Bhattacharjee-Reply, ¶184.

First, the ’116 specification expressly says that “the invention is not intended to be limited” to a particular data splitting process, but rather that POSAs “will recognize...a wide number of alternatives for the data splitting process” (21:44-48), and that “data may be split into *any desired*” data unit size (21:55-59), including data units that are “all of the same size” (21:65-66). Thus, the ’116 patent explicitly allows for *data chunks* to be any subset of the *data set*. Bhattacharjee-Reply, ¶¶184-190. Rubin-Depo., 17, 157-158.

Second, contrary to SFI’s allegation that Foster’s payloads are “not created to protect the data” (POR, 22), Foster discloses dividing the content into content units so that each payload can be encrypted with a different encryption key to “provide enhanced security by preventing an entire content stream from being accessed with

a single key” (Foster, [0004], [0071]). Petition, 52; Bhattacharjee-Reply, ¶¶191-193. Moreover, Foster-Hayhurst applies Hayhurst’s distributive storage to “provide[] a high level of security and a deterrence to piracy.” Hayhurst, [0008]; Petition, 62-64. Thus, both Foster and Foster-Hayhurst divide Foster’s content into packet payloads expressly to protect the data. Bhattacharjee-Reply, ¶194.

SFI also points to “literature” that refers to “a packet or packet payload...itself being divided into ‘chunks.’” POR, 20-21. That evidence *supports* that a *data chunk* is just a data unit smaller than the data on which “chunking” is performed. Further, that Foster’s payload packets are *data chunks* is reinforced by literature referring to a “packet” as a “chunk” of a larger data set. Bhattacharjee-Reply, ¶¶195-201 (citing EX1082, 8; EX1083, 7:33-40; EX1084, [0026]; EX1085, 4:7-25).

Respectfully submitted,

Date: 12-23-2024

/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 5,561 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.