

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

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. PETITIONER’S TAJIMA GROUND FAILS (GROUND 1; CLAIMS 1, 5-8).....	1
III. PETITIONER’S TAJIMA/FOSTER, TAJIMA/RIVEST AND TAJIMA/RIVEST/SHYU GROUNDS FAIL (GROUNDS 2, 3 AND 4; CLAIMS 1-3, 6, 9-14).	8
A. Petition Fails To Show A Motivation To Combine Tajima/Foster With A Reasonable Likelihood Of Success (Ground 2; Claims 1-2, 9, 11-14).	9
1. Petitioner Fails To Demonstrate That A POSITA Would Be Motivated to Combine Tajima and Foster In The Normal Course Of Research And Development.	9
2. Petitioner Fails To Prove A POSITA Would Be Motivated to Combine Tajima and Foster.....	16
B. Petitioner Fails To Show A Motivation To Combine Tajima/Rivest (Ground 3; Claims 9-14).	28
C. Petitioner Fails To Show A Motivation To Combine Tajima/Rivest/Shyu (Ground 4; Claims 1-3, 6).	32
D. Petitioner’s Tajima Combinations Are Hindsight-Driven And Do Not Consider Their Drawbacks.....	35
IV. THE FOSTER-HAYHURST GROUND FAILS (GROUND 5, CLAIMS 1-2, 5, 9 AND 11).....	38
A. Petitioner Fails To Demonstrate That Hayhurst Is Analogous Art.	38
1. Hayhurst And The ’116 Patent Do Not Share The Same Field Of Endeavor.	39

	<u>Page</u>
2. Hayhurst Is Not Reasonably Pertinent to the Problem the Inventors of the '116 Patent Were Addressing.....	44
B. Petitioner Fails To Demonstrate That A POSITA Would Be Motivated To Combine Foster And Hayhurst.....	47
1. Foster Provides Synchronized Transmission To Avoid Delays.....	48
2. Hayhurst's Goal Is Directed to Reducing the Bandwidth Requirements for the Provision of Content Where Immediate, Random Access Is Not Required.....	53
3. Petitioner's Combination Involves Storing and Distributing All of Foster's Content Units per Hayhurst's Method.....	55
4. A POSITA Would Not Be Motivated To Combine Foster And Hayhurst As Proposed.....	56
C. Petitioner's Foster-Hayhurst Combination Fails Because Neither Foster Not Hayhurst Disclose "Data Chunks."	68
CONCLUSION.....	70

TABLE OF AUTHORITIES

Cases

<i>Airbus S.A.S. v. Firepass Corp.</i> , 941 F.3d 1374 (Fed. Cir. 2019)	40
<i>Apple Inc. v. Cellular Comm’ns Equipment, LLC</i> , IPR2015-00576, Paper 7 (June 12, 2015).....	25
<i>Arctic Cat Inc. v. Polaris Indus.</i> , 795 Fed. App’x. 827 (Fed. Cir. 2019)	35, 56
<i>AstraZeneca AB v. Mylan Pharm. Inc.</i> , 19 F.4th 1325 (Fed. Cir. 2021)	27
<i>In re Bigio</i> , 381 F.3d 1320 (Fed. Cir. 2004)	40
<i>BlephEx, LLC v. Myco Indus., Inc.</i> , 24 F.4th 1391 (Fed. Cir. 2022)	5
<i>In re Clay</i> , 966 F.2d 656 (Fed. Cir. 1992)	39, 43, 44, 47
<i>In re Conrad</i> , 759 Fed. App’x. 982 (Fed. Cir. 2019)	38
<i>DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.</i> , 567 F.3d 1314 (Fed. Cir. 2009)	27
<i>Dish Network LLC v. Entropic Comm’s</i> , IPR2024-00560, Paper 11 (P.T.A.B. August 15, 2024)	23
<i>Donner Tech., LLC v. Pro Stage Gear, LLC</i> , 979 F.3d 1353 (Fed. Cir. 2020)	44
<i>DSS Tech. Mgm’t v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	6
<i>Everstar Merch. Co. v. Willis Elec. Co.</i> , No. 2021-1882, 2022 WL 1089909 (Fed. Cir. Apr. 12, 2022).....	35

	<u>Page</u>
<i>F5 Networks, Inc. v. Radware, Ltd.</i> , IPR2017-00124, Paper 48, 64-65 (Apr. 23, 2018)	25
<i>In re Gordon</i> , 733 F.2d 900	57
<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016)	4
<i>In re ICON Health & Fitness, Inc.</i> , 496 F.3d 1374 (Fed. Cir. 2007)	57
<i>Intel Corp. v. Qualcomm Incorp.</i> , 21 F.4th 784 (Fed. Cir. 2021)	35
<i>InTouch Techs., Inc. v. VGo Commc'ns., Inc.</i> , 751 F.3d 1327 (Fed. Cir. 2014)	8, 38
<i>Kamstrup A/S v. Axioma Metering UAB</i> , 43 F.4th 1374 (Fed. Cir. 2022)	40
<i>In re Klein</i> , 647 F.3d 1343 (Fed. Cir. 2011)	44
<i>Microsoft Corp. v. Biscotti, Inc.</i> , 878 F.3d 1052 (Fed. Cir. 2017)	3
<i>In re NTP, Inc.</i> , 654 F.3d 1279 (Fed. Cir. 2011)	24
<i>Plas-Pak Indus., Inc. v. Sulzer Mixpac AG</i> , 600 F. App'x. 755 (Fed. Cir. 2015)	7, 57
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	7
<i>Polygroup Ltd. v. Willis Elec. Co., Ltd.</i> , IPR2016-01610, Paper 187, 31, 35-40 (Feb. 26, 2018)	47
<i>In re Ratti</i> , 270 F.2d 810 (CCPA 1959)	57

Page

<i>Ruiz v. A.B. Chance Co.</i> , 357 F.3d 1270 (Fed. Cir. 2004)	8, 38
<i>Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.</i> , 66 F.4th 1373 (Fed. Cir. 2023)	39
<i>Tec Air, Inc. v. Denso Mfg. Mich., Inc.</i> , 192 F.3d 1353 (Fed. Cir. 1999)	57
<i>Trintec Indus., Inc. v. Top U.S.A. Corp.</i> , 295 F.3d 1292 (Fed. Cir. 2002)	3
<i>Unigene Labs., Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	10
<i>Univ. of Strathclyde v. Clear-Vu Lighting LLC</i> , 17 F.4th 155 (Fed. Cir. 2021)	37
<i>Quectel Wireless Sols. Co.</i> , 2024 WL 3665345 (Fed. Cir. Aug. 6, 2024)	35
<i>Wang Labs., Inc. v. Toshiba Corp.</i> , 993 F.2d 858 (Fed. Cir. 1993)	43, 47
<i>Winner Int’l Royalty Corp. v. Wang</i> , 202 F.3d 1340 (Fed. Cir. 2000)	35
<i>In re Wood</i> , 599 F.2d 1032 (CCPA 1979)	40
<i>Wyers v. Master Lock Co.</i> , 616 F.3d 1231 (Fed. Cir. 2010)	40

EXHIBIT LIST	
2001	Reserved
2002	Reserved
2003	Declaration of Aviel D. Rubin, Ph.D.
2004	Reserved
2005	Bruce Schneier Curriculum Vitae [Schneier-CV]
2006	Bruce Schneier, <i>Why Cryptography Is Harder Than It Looks</i> , SCHNEIER ON SECURITY, 1997, https://www.schneier.com/essays/archives/1997/01/why_cryptography_is.html [Schneier-Why-Cryptography-Is-Harder-Than-It-Looks]
2007	Excerpts from Jonathan Katz et al., <i>Introduction to Modern Cryptography</i> (1st ed. 2007) [Katz]
2008	Bruce Schneier, <i>Security Pitfalls in Cryptography</i> , SCHNEIER ON SECURITY, 1998, https://www.schneier.com/essays/archives/1998/01/security_pitfalls_in.html [Schneier-Security-Pitfalls-in-Cryptography]
2009	Excerpts from Ross Anderson, <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i> (1st ed. 2001) [Anderson]
2010	Excerpts from Bruce Schneier, <i>Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C</i> (2nd ed. 2015) [Schneier-Applied-Cryptography]
2011	Patent Application Publication to Tsai US 2005/0195857 A1 [Tsai]
2012	Edgar Pek et al., <i>Formal Verification of Communication Protocols in Distributed Systems</i> , SYMPOSIUM ON OPERATING SYS. PRINCIPLES, 2003 [Pek]

2013	Jan Friso Groote et al., <i>A Bounded Retransmission Protocol for Large Data Packets: A Case Study in Computer Checked Algebraic Verification</i> , 1996 [Groote]
2014	Microsoft, <i>Overview of MPEG-2 Systems</i> , WWW.LEARN.MICROSOFT.COM , July 27, 2023, https://learn.microsoft.com/en-us/windows/win32/directshow/overview-of-mpeg-2-systems [Overview-of-MPEG-2-Systems]
2015	Excerpts from Harry Newton, <i>Newton's Telecom Dictionary</i> (16th ed. 2000) [Newton's-Telecom-Dictionary]
2016	Excerpts from <i>Oxford Dictionary of Computing</i> (1996) [Oxford-Dictionary-of-Computing]
2017	IBM, <i>Transmission Control Protocol (TCP)</i> , WWW.IBM.COM , https://www.ibm.com/docs/en/zos-basic-skills?topic=4-transmission-control-protocol-tcp [IBM]
2018	<i>Security First Innovations, LLC v. Google LLC</i> , 2:23-cv-00091 (JKW-RJK), Google's Opening Claim Construction Brief (December 6, 2023) [Google's-Opening-Claim-Construction-Brief]
2019	Excerpts from Microsoft Press, <i>Microsoft Computer Dictionary</i> (5th ed. 2002) [Microsoft-Computer-Dictionary]
2020	<i>Security First Innovations, LLC v. Google LLC</i> , 2:23-cv-00091 (JKW-RJK), Google's Responsive Claim Construction Brief (Jan. 8, 2024) (Non-Confidential Redacted Version) [Google-Responsive-Claim-Construction-Brief]
2021	Cambridge Dictionary, <i>Set-Top Box</i> , https://dictionary.cambridge.org/us/dictionary/english/set-top-box (last visited Feb. 27, 2024)

2022	Jim Connors, INFOWORLD, <i>The evolution of cable television to interactive communications service provider</i> (Oct. 1, 1996), https://www.infoworld.com/article/2077255/the-evolution-of-cable-television-to-interactive-communications-service-provider.html [InfoWorld]
2023	Excerpts from Oxford University Press, Oxford English Dictionary (12th ed. 2012) [Oxford-English-Dictionary]
2024	Excerpts from HarperCollins Publishers, English Dictionary for Advanced Learners (3d ed. 2001) [Collins-Dictionary]
2025	Japanese Patent Application Publication No. JP2003046500A to Tajima et al. [Tajima-Japan-Application]
2026	Cambridge Dictionary, 登録, https://dictionary.cambridge.org/us/dictionary/japaneseenglish/%E7%99%BB%E9%8C%B2 (last visited Mar. 22, 2024) [Cambridge-Japanese-English-Dictionary]
2027	TechTarget, Certificate Authority, https://www.techtarget.com/searchsecurity/definition/certificateauthority (last updated Sept. 2021) [TechTarget]
2028	Declaration of Colette Woo [SERVED, NOT FILED]
2029	Jonathan Katz et al., <i>Introduction to Modern Cryptography</i> (1st ed. 2007) [SERVED, NOT FILED]
2030	Cambridge Dictionary, 登録, https://dictionary.cambridge.org/us/dictionary/japanese-english/%E7%99%BB%E9%8C%B2 (last visited June 17, 2024) [SERVED, NOT FILED]

2031	Ross Anderson, <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i> (1st ed. 2001) [SERVED, NOT FILED]
2032	Bruce Schneier, <i>Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C</i> (2nd ed. 2015) (E-Book) [SERVED, NOT FILED]
2033	Second Declaration of Dr. Aviel D. Rubin in Support of Patent Owner's Response [Rubin-2nd-Decl.]
2034	Deposition Transcript of Dr. Samrat Bhattacharjee, taken on August 9, 2024 [Bhattacharjee-Depo.]
2035	C. Patrikakis et al., <i>Streaming Content Wars: Download and Play Strikes Back</i> , UCMedia 2009, LNICST 40, pp. 218–226, 2010. [Patrikakis]
2036	J. Hur et al., <i>Packet Chunking for File Detection</i> , IEEE/ACM Transactions on Networking Vol. 31 (2023). [Hur]
2037	R. Li et al., <i>A Framework for Qualitative Communications Using Big Packet Protocol</i> , 2019, https://doi.org/10.48550/arXiv.1906.10766 . [Li]
2038	N. McKeown et al., <i>The Tiny Tera: A Packet Switch Core</i> , IEEE Micro 17, 1998. [McKeown].
2039	<i>Marlin DRM FAQ</i> , Marlin Community, https://www.marlin-community.com/faq/ (last accessed Sept. 9, 2024) [Marlin-DRM].
2040	<i>What is Conditional Access?</i> , Verimatrix anti-piracy (Aug. 1, 2023), https://www.verimatrix.com/anti-piracy/knowledge-base/what-is-conditional-access/ [Verimatrix].
2041	R. Li et al., <i>New IP: A Data Packet Framework to Evolve the Internet</i> , 2020, https://www.researchgate.net/publication/341582478 [Li-II]

I. INTRODUCTION

Petitioner fails to prove that any challenged claim is invalid. Petitioner's Tajima ground (Ground 1) fails because Petitioner fails to prove that Tajima teaches the limitation of the independent claims directed to "storing each data chunk...together with one of the plurality of obfuscated different encryption keys." Its Tajima/Foster (Ground 2), Tajima/Rivest (Ground 3), and Tajima/Rivest/Shyu (Ground 5) combinations fail because Petitioner fails to prove that a POSITA would be motivated to make its proffered hindsight driven combinations with a reasonable expectation of success. Petitioner's Foster-Hayhurst combination (Ground 5) fails because Petitioner fails to prove that Hayhurst is analogous art, that a POSITA would be motivated to make the combination, or that Foster-Hayhurst teaches all of the limitations of the independent claims.

II. PETITIONER'S TAJIMA GROUND FAILS (GROUND 1; CLAIMS 1, 5-8).

Independent claim 1, from which claims 5-8 depend, requires "storing each data chunk...together with one of the plurality of obfuscated different encryption keys." EX1001 cl. 1. In each of its Tajima-based grounds, Petitioner argues that Tajima discloses and/or renders obvious this limitation by teaching attaching "information regarding the key" (also called "key information" by Tajima) to the data fragments. Pet., 20-22, 24 ("Tajima separately stores each encrypted data

fragment together with an ‘obfuscated different encryption key’ (*i.e.*, the key information that encrypted the other data fragment) on ‘a plurality of different storage devices’ (*i.e.*, a plurality of different databases...)” (emphasis in original); *see also, id.*, 40-41, 43, 47 and 49. However, Tajima does not state or suggest that the key itself is encompassed by “information regarding the key,” and what Tajima does disclose indicates it is not. Petitioner argues obviousness in the alternative, but presents only a conclusory, hindsight driven analysis.

Petitioner concedes that it relies upon Tajima’s disclosure, in connection with the embodiments in Figures 12 and 13 of the reference, that “information regarding the key that was used for the encryption” is attached to a data fragment, rather than the key itself:

Fig. 12

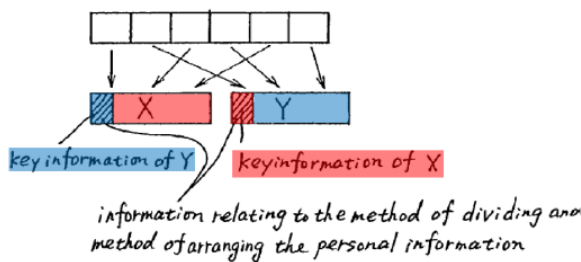
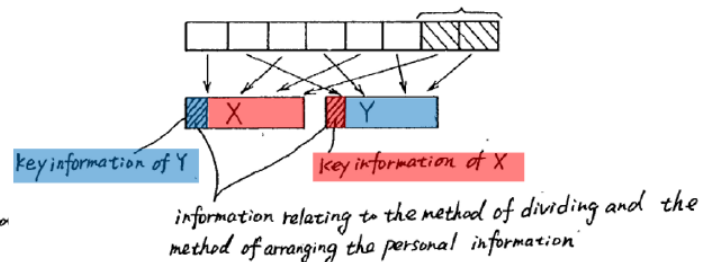


Fig. 13



Pet., 19 (citing EX1005 Figs. 12, 13); [0112]; [0114] (same). Acknowledging that Tajima does not explicitly disclose that “information regarding the key” includes the key itself, Petitioner argues that “**POSAs understood** that Tajima’s ‘key information’—*i.e.*, ‘information regarding the key that was used for the encryption

of [the respective] data fragment’ (Tajima, [0111], [0113])—includes at least the corresponding key.” Pet., 20 (citing only EX1003 ¶ 96).¹ To show anticipation by Tajima, Petitioner’s claim about what a POSITA “understood” must meet the requirements for an inherent disclosure. *Microsoft Corp. v. Biscotti, Inc.*, 878 F.3d 1052, 1065 (Fed. Cir. 2017) (statements that “a [POSITA] would understand the [evidence] as disclosing [the limitation]” could support an argument that a limitation was “inherently disclose[d] ...”). Inherency requires demonstrating that a limitation is “‘necessarily present,’ not merely probably or possibly present, in the prior art.” *Trintec Indus., Inc. v. Top U.S.A. Corp.*, 295 F.3d 1292, 1295 (Fed. Cir. 2002). But Petitioner fails to demonstrate that “information regarding the key” would “necessarily” include the key. As Dr. Rubin explains:

I do not believe that a POSITA would understand that Tajima uses the term “information regarding the key” to refer to the key. If Tajima meant to say the “key,” there would be no need to use the phrase “information regarding the key.”

When Tajima wishes to refer to a “key,” it does so directly and, indeed, there are numerous instances where Tajima refers to, *e.g.*, a “public key” or a “secret key.” []

¹ All emphasis added unless otherwise noted.

Thus, Tajima appears to use the term “key” when it means a key, and uses the terms “key information” or “information **regarding the** key” to refer to some type of information about the key, not to the key itself.

EX2033 ¶¶ 41-43 (citing EX1005 [0067], [0070], [0071], [0075], [0077], [0086], [0088], [0089].)

Petitioner acknowledges that “Tajima never says...anything” about what constitutes information regarding the key, but argues that because it “does not disclose” a “separate key management” system, “the key information includes the key.” Pet., 20-21. Tajima’s silence does not compel the inference Petitioner suggests. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363-64 (Fed. Cir. 2016) (rejecting reliance on “unsupported and inferential theories” in absence of “express teaching”). As Dr. Rubin explains:

Petitioner and Dr. Bhattacharjee seem to be relying upon Tajima’s silence regarding key management, arguing that information regarding the key includes the key itself because Tajima “does not disclose any additional steps nor any separate key management infrastructure.” This conclusion does not logically follow. All Tajima discloses is that “information regarding the key” is stored with the data fragment. It is silent about what key information is and where the key itself is stored.

Petitioner also relies on Tajima’s statements that “information regarding the key” “is used to decrypt” a data fragment. EX1005 [0112], [0114]. But that does not establish that the key itself is **stored**

with the data fragment. If the information regarding the key indicates, *e.g.*, the type of key that is used, or information that can be used to derive the key, such information could be “used to decrypt” a data fragment without being the key itself.

EX2033 ¶ 45-46.

Petitioner also argues that key information includes the key itself because one of Tajima’s claims (which Petitioner alleges is directed to a Figure 11 embodiment) recites an “encryption key” where Figure 11 recites “key information.” Pet., 21. But the Figure 11 embodiment does not encrypt data fragments, and thus cannot disclose where the keys used to encrypt data fragments are stored. Moreover, Petitioner does not rely on Tajima’s Figure 11 embodiment, and so Tajima’s alleged disclosures regarding that embodiment have no bearing on whether the Figure 12 and 13 embodiments (that Petitioner **does** rely on) necessarily disclose attaching the keys used to encrypt the fragments to the fragments themselves. “‘It is not enough that the prior art reference...includes multiple, distinct teachings that the artisan might somehow combine to achieve the claimed invention’ to show anticipation.” *BlephEx, LLC v. Myco Indus., Inc.*, 24 F.4th 1391, 1400 (Fed. Cir. 2022).

Alternatively, Petitioner argues that it would have been obvious to include the key itself in “information about the key.” Pet., 22 (citing EX1003 ¶ 104). But beyond Dr. Bhattacharjee’s conclusory testimony, which has no support in Tajima,

Petitioner offers no evidence or explanation as to why this “would have been an obvious and conventional way” to modify Tajima. To the extent Petitioner relies on the purported “common sense” of a POSITA, that be used to supply a missing limitation “**only** when ‘the limitation in question [is] unusually simple and the technology particularly straightforward.’” *DSS Tech. Mgm’t v. Apple Inc.*, 885 F.3d 1367, 1374 (Fed. Cir. 2018) (citations omitted). The complexity and risks associated with modifying cryptographic systems bar such an argument. (See EX2033 ¶ 48).

As Dr. Rubin explains:

Petitioner’s proposed modification to Tajima involve where and how to store encryption keys and thus cannot be merely “conventional.” Rather, these choices must be carefully considered and the threat model properly assessed because key management is the most difficult and most vulnerable part of cryptography. See EX2010 169 (“In the real world, key management is the hardest part of cryptography.”); EX2008 (“And just as it’s possible to build a weak structure using strong materials, it’s possible to build a weak cryptographic system using strong algorithms and protocols.”); EX2009 [Anderson] (new computer “security systems have a nasty habit of backfiring”).

EX2033 ¶49. Petitioner’s reliance solely on a POSITA’s “common sense” should be rejected.

Nor does Petitioner demonstrate a POSITA would be motivated to make the proposed alteration. As Petitioner acknowledges, a POSITA would understand there

are significant security drawbacks to including the encryption key itself in the “key information” because “[i]t was known that storing plaintext (i.e., unencrypted) keys with encrypted data results in a vulnerability.” Pet., 33-34; EX1003, ¶140, *citing, e.g.,* EX1021, 1:45-65 (explaining that methods “where the data encryption keys are stored or transmitted together with the encrypted data” are potentially defeatable). Encrypting the data fragment encryption key with yet another key before storing it with the fragment would require additional key management, contrary to what the Petition asserts as Tajima’s goal: “a system that needs only the key information to decrypt data fragments and not additional key management infrastructure.” See Pet., 22; *contra Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1069-70 (Fed. Cir. 2018) (no find motivation where combination “would run contrary to [reference’s] stated purposes.”); *Plas-Pak Indus., Inc. v. Sulzer Mixpac AG*, 600 F. App’x. 755, 759 (Fed. Cir. 2015) (“[A] change in a reference’s ‘principle of operation’ is unlikely to motivate a [POSITA] to pursue a combination with that reference.”) (non-precedential).

Petitioner’s obviousness theory should be rejected as no more than an attempt to convert Tajima’s silence on where its data fragment encryption keys are stored into a feature of Tajima that, Petitioner claims, happens to encompass a limitation in claim 1 of the ’116. This is the quintessential hindsight-driven analysis the Federal

Circuit has rejected. *Ruiz v. A.B. Chance Co.*, 357 F.3d 1270, 1275 (Fed. Cir. 2004) (rejecting “hindsight reasoning, using the invention as a roadmap to find its prior art components” to show obviousness); *InTouch Techs., Inc. v. VGo Commc’ns., Inc.*, 751 F.3d 1327, 1351 (Fed. Cir. 2014) (rejecting expert’s obviousness theory that “relied on the [] patent itself as her roadmap for putting what she referred to as pieces of a ‘jigsaw puzzle’ together.”).

III. PETITIONER’S TAJIMA/FOSTER, TAJIMA/RIVEST AND TAJIMA/RIVEST/SHYU GROUNDS FAIL (GROUNDS 2, 3 AND 4; CLAIMS 1-3, 6, 9-14).

Five of the challenged claims require “transforming each of the plurality of different encryption keys” which were used to “encrypt[] each of the data chunks.” *E.g.*, EX1001 cl. 9. Petitioner does not dispute that Tajima does not teach “transforming each of the plurality of different encryption keys” under either parties’ construction.² Rather, Petitioner proposes combining Tajima with Foster to allegedly meet Patent Owner’s construction of “transforming” (Pet., 6-7) and Tajima with Rivest to allegedly satisfy Petitioner’s construction of the term (*id.*, 6).

² Petitioner asserts that the combination of Foster and Tajima also discloses “obfuscating” a key, as required by claim 1, under Patent Owner’s district court construction.

Petitioner also adds Shyu to Tajima and Rivest to meet its construction of “data indicative of at least one of ...the encryption keys.” The Petition fails to offer any legitimate reason to combine these references, ignores the drawbacks of its proposed combinations, and relies on hindsight to combine disparate references to mimic the ’116’s inventive path.

A. Petition Fails To Show A Motivation To Combine Tajima/Foster With A Reasonable Likelihood Of Success (Ground 2; Claims 1-2, 9, 11-14).

1. Petitioner Fails To Demonstrate That A POSITA Would Be Motivated to Combine Tajima and Foster In The Normal Course Of Research And Development.

Obviousness requires a showing that a POSITA “would have selected and combined [the] prior art elements in the normal course of research and development to yield the claimed invention.” *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Petitioner, however, fails to demonstrate that its Tajima/Foster combination meets this fundamental requirement.

As Dr. Rubin explains, Tajima and Foster are directed to entirely different fields and to different problems, and in the normal course of research and development would not have considered combining the two references:

Tajima “relates to a personal information management system” and improves upon a prior art “online shopping system” and prior art “public key cryptosystem” with a certificate authority. See EX1005

[0001], [0004]-[0007], [0025], [0042]. Thus, Tajima teaches that “an object of” its invention is to “improve the security of personal information.” *Id.*, 44. More specifically, Tajima addresses “online shopping” wherein “a user purchases goods” and “the payment method[] and the content of the customer information” including “the user’s name, address, telephone number, and e-mail address” must be provided to the store. *Id.*, [0004]-[0007].

EX2033 ¶54.

In the Figure 12 and 13 embodiments of Tajima’s system on which Petitioner relies, a dataset comprising a user’s personal information is divided into multiple (at least two) “data fragments.” Pet., 15. The fragments, indicated as “X” and “Y” are each encrypted using a different key. *Id.* 18 (citing EX1005, [0111], [0113].

Fig. 12

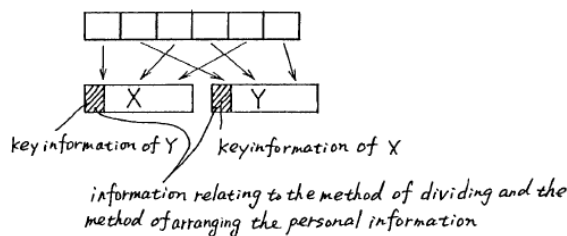
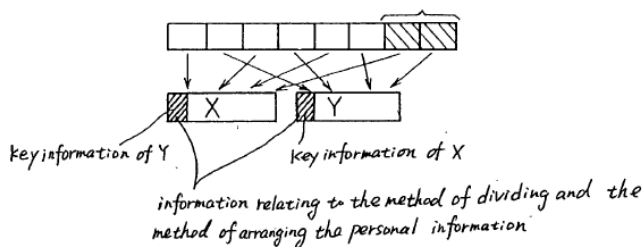


Fig. 13



Tajima states that after they are encrypted, “[i]nformation regarding the key that was used for the encryption of data fragment Y is attached to encrypted data fragment X, and information regarding the key that was used in the encryption of data fragment X is attached to encrypted data fragment Y.” ***Thus, in Tajima’s method each chunk is attached to information regarding a key that cannot decrypt that chunk.*** EX 1005, [0111]-[0114]. Data fragment X (with attached key information for fragment Y) is then “registered” (allegedly, stored) with a different certificate authority than fragment Y (which is stored along with attached key information for fragment X).

Foster, by contrast, discloses a system wherein a content owner (*e.g.*, a movie studio) provides content to Foster’s system for encryption and immediate transmission (*e.g.*, streaming via the internet) to a recipient.

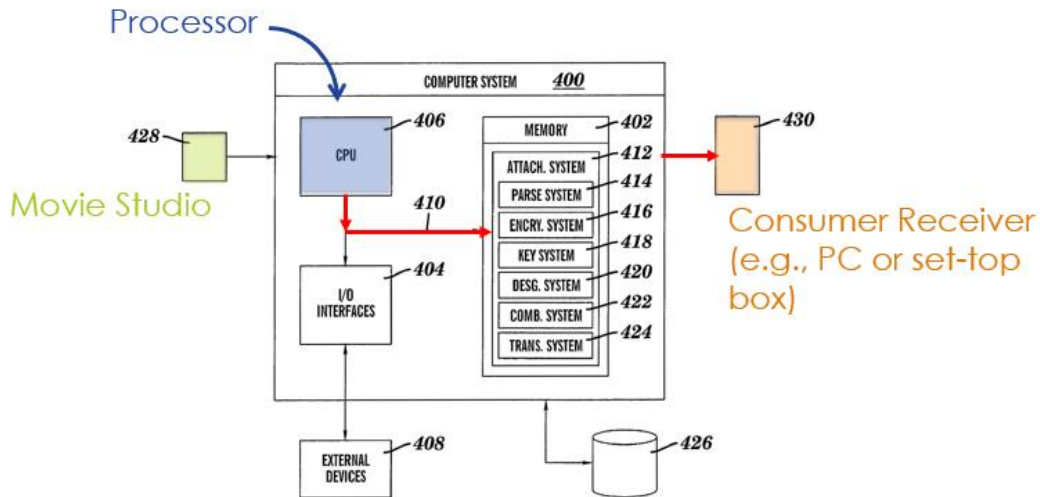


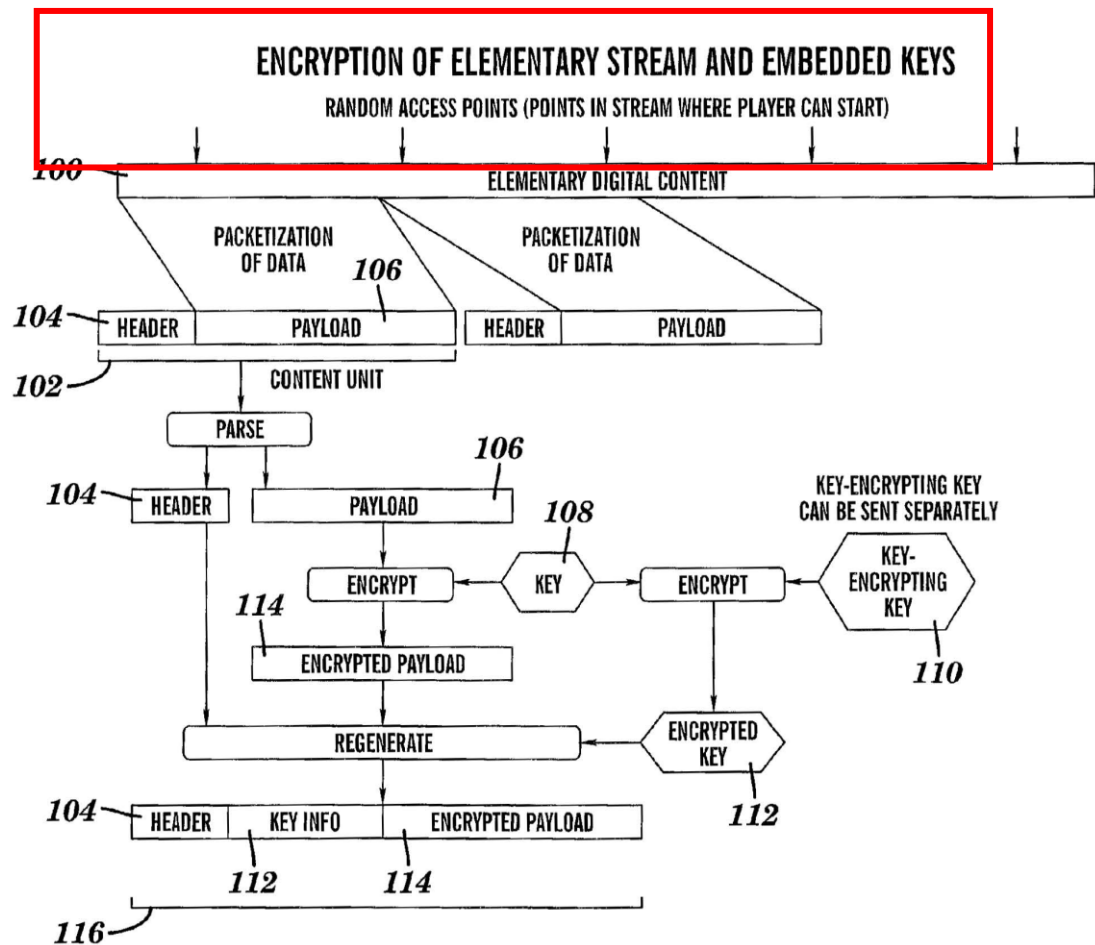
FIG. 16

See EX1006 Fig. 16 (annotated); [0002] (“system ... for attaching a title key to encrypted content for synchronized transmission to a recipient.”); [0078] (“computer system 400...process[es] content units of an elementary content stream” for “transmi[ssion]...to a recipient”).

Foster’s system processes and transmits data packets (“also called content units”) between a “content service provider” “such as a cable service provider” (*id.*, [0039]) and a “receiver” “such as a set-top box” (*id.*, [0040]). *Id.*, Fig. 16, [0078]. It seeks to improve upon prior art cable systems providing real-time television. *Id.*, [0052] (Foster is directed towards “Conditional Access System[s] (CAS),” which are “cable or satellite television system[s]”); [0006]. As Dr. Rubin explains,

Foster's innovations are primarily useful in the streaming context, where the individual content units are serial components of a real-time content stream:

Foster's teachings of synchronized transmission are primarily significant in a streaming context contemplated by Foster's Figure 8, which Petitioner relies upon (*e.g.*, Pet., 56, 65-66). "In streaming, multimedia data is transferred in a stream of packets that are interpreted and rendered in real time by a software application, as the packets arrive in the user's terminal." EX2035 [Patrikakis] 220. Because packets are transmitted as a stream and rendered in real-time, any delays have an especially noticeable impact. When watching, *e.g.*, a live sporting event, any delay in receiving, decrypting and/or rendering each content unit in a stream would be a significant drawback. Figure 8 depicts the "Encryption of [an] Elementary Stream," provided to a set-top box which has "random access points (points in stream where player can start [displaying the stream])":

**FIG. 8**

EX1006 Fig. 8; *see also id.*, [0064]. Foster teaches that when content and keys are not sent synchronously, random access of content as contemplated by its Figure 8 embodiment “is not possible.” *Id.*, [0063]; *see also id.*, [0064], [0071].

EX2033 ¶122.

To facilitate streaming, *Foster's system requires synchronizing the transmission of encrypted content packets with the keys used to encrypt those packets*, so that each packet can be viewed immediately upon receipt. This fundamental goal is reflected in Foster's title, abstract, field of the invention, background of the invention, summary of the invention, and its disclosure generally. By "synchronized" transmission, Foster means specifically that the keys used to encrypt the content packets "are...attached to the corresponding encrypted content packets." See, e.g., EX1006, Abstract.

Thus, in contrast to Tajima's disclosure that its title key is secured by attaching it to a *different* data fragment, the problem Foster sought to solve is the "need...for a key used to encrypt content to be itself encrypted, and transmitted as an integral part of the [same] content." *Id.*, [0007]. Foster solves this problem by doing the opposite of Tajima—by attaching each encryption key to the packet it can decrypt. Foster explains that

[s]pecifically, under the present invention, a content unit including a content packet and a header is received and parsed. A title key is then used to encrypt the content packet. Once the content packet is encrypted, the title key is itself encrypted with a key encrypting key. The encrypted title key is then attached to the content packet and the header for synchronized transmission to, or storage by a receiver.

Id., [0008]. Foster is designed to improve upon prior art systems susceptible to “loss of synchronization between the content and the keys.” EX1006, [0006]. Confirming its importance in Foster, at his deposition Dr. Bhattacharjee stated that “synchronous transmission [of key and content] to a receiver” was “sort of the whole invention in Foster.” EX2034, 32:20-23.

In short, Tajima and Foster address different problems in different fields using methods that are fundamentally at odds. In the normal course of research and development, no POSITA would have thought to combine these references. As Dr. Rubin explained

In my opinion, Tajima and Foster are far afield of one another, arise in manifestly different environments and confront quite different problems. I do not believe a POSITA would have naturally combined Tajima and Foster in the normal course of research and development.

EX2033 ¶62.

2. Petitioner Fails To Prove A POSITA Would Be Motivated to Combine Tajima and Foster

Petitioner contends that a POSITA would combine Tajima and Foster by using Tajima’s disclosure of “dividing personal information and securely storing data fragments on [different] databases” with “Foster’s key-encryption technique.” Pet., 37-38. Specifically, Petitioner asserts that the combination would “store each data fragment” created by Tajima’s method; each data fragment would be encrypted with

a key. Invoking Foster, Petitioner asserts that this key would be encrypted with a key encryption key. Petitioner proposes that this “encrypted key information” would then be stored with a data fragment that it cannot be used to decrypt; in other words, the key information would be stored with a data fragment other than the one it was used to encrypt, as the Petition claims is true in Tajima . *See* Pet., 45. Petitioner claims that a POSITA “would have recognized the desirability of using Foster’s key-encryption technique to encrypt Tajima’s keys before attaching them to different encrypted fragments” to benefit from a purported “increased level of security.” Pet., 37. Petitioner also claims that the POSITA “would have realized that this benefit would be achieved with little modification to Tajima’s system.” *Id.*

Contrary to Petitioner’s claim, combining Tajima and Foster would be neither easy nor beneficial, and a POSITA would not be motivated to make the combination proposed by Petitioner, or have any reasonable expectation of success in doing so. A POSITA would not be motivated to combine these references because (1) Tajima and Foster lack critical disclosures, precluding their combination; (2) application of the key encryption key (“KEK”) technique of Foster to secure Tajima’s key information would render Tajima’s own method of securing key information redundant; and (3) the combination proposed by Petitioner would be contrary to Foster’s primary goal of keeping the key with the content it can decrypt.

- (a) *A POSITA Would Not Be Motivated to Combine Tajima and Foster Because They Lack Key Disclosures, and Using Foster Would Make Tajima's Key-Securing Technique Redundant.*

A POSITA would not be motivated to, or have a reasonable expectation of success in, combining Tajima with Foster to create the inventions of independent claims 1 or 9 of the '116, or any of the dependent claims. Each reference is silent about a key feature of those inventions, consequently, it is unclear **how** a POSITA could combine the references with a reasonable expectation of success in achieving the claimed inventions. Moreover, applying the key encryption technique of Foster to Tajima's key information would render the technique Tajima already uses to secure that information redundant.

- (i) *Tajima and Foster Each Fail to Disclose a Feature of the Claimed Invention.*

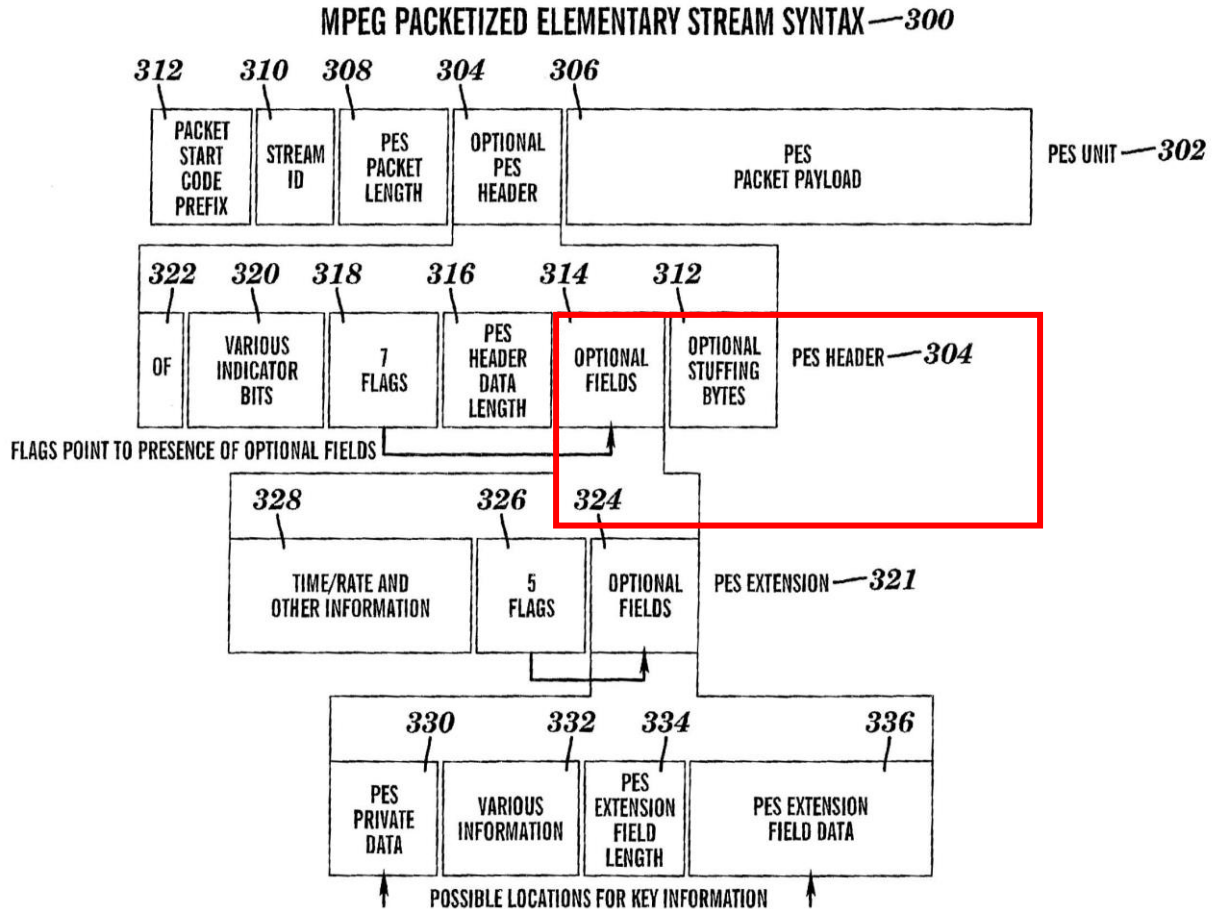
While Tajima discloses dividing a dataset into data fragments corresponding to the claimed data chunks, it only discloses attaching "information regarding the key" to those data fragments. As explained above, Tajima **does not disclose attaching the key itself to a data fragment**. See *supra* Section II.A.

Foster, as explained below, operates on MPEG video packet payloads and **does not disclose generation of data chunks**. Further, it requires that **the key** itself be attached to the packet it decrypts

Limitations [1A] and [9A] require “distributing the data set into a plurality of data chunks.” Petitioner fails to show that Foster’s “content units,” which are MPEG video packet payloads, are the claimed “data chunks” or that a POSITA would understand that the content units correspond to Tajima’s data fragments. As Dr. Rubin explains:

Petitioner and Dr. Bhattacharjee rely on a correspondence between Tajima’s data fragments and Foster’s packet “payloads” as the claimed data chunks. Pet., 36. But Foster teaches that these “payloads” refer to the payloads of MPEG Packetized Elementary Stream (PES) packets (also referred to in Foster as “content units”), as illustrated in Foster’s Figure 13. See EX1006 Fig. 13; *see also id.*, [0072] (“a MPEG packetized elementary stream 300 is parceled into PES (packet) units 302....PES unit 302 includes packetized elementary stream (PES) packet payload 306” which “will be encrypted with a title key”). Unlike the “data chunks” described in the ’116, these payloads do not exist to protect the data.

EX2033 ¶68.



There is no reason to assume that a POSITA would understand that Foster's packet payload corresponds to the data chunk of the '116 or the data fragment of Tajima. As Dr. Rubin explains, the literature frequently refers to a packet or packet payload as something that is itself divided into "chunks" or fragments:

Consistent with the fact that they are not intended to protect data, numerous technical articles refer to a packet or packet payload itself being divided into chunks or fragments. *See, e.g.,* EX2036 1202 ("The

new scheme uses a content-based chunking algorithm to consistently divide both files and packet payloads into multiple byte sequences, called chunks.”); EX 2037 1 (“These services allow breaking down packet payloads into smaller units (called chunks) ...”); *see also id.*, 2 (“It provides a packetization method that breaks down the payload into multiple chunks, each with a certain significance.”); EX2012, 3 (“[The d]ata packet is delivered as a sequence of chunks.”); EX2013 (“the input is a large data packet ... which is delivered in small chunks.”); EX2038 4-5 (“A packet consists of multiple chunks...); EX2041, 7 (“the payload could be divided into multiple equal-sized chunks...”).

EX2033 ¶71.

Moreover, the difference between the claimed “data chunks” or Tajima’s data fragments and Foster’s packet payloads is significant. As Dr. Rubin explains, whereas the ’116’s data chunks and Tajima’s data fragments are generated to further secure the data, Foster’s packet payloads are merely a by-product of the MPEG streaming standard:

As the ’116 explains, partitioning the data set into chunks increases security because when “data...remains whole and intact,” it is “subject to attack.” The ’116 addresses this concern, in part, by “performing a cryptographic parsing and splitting of the encrypted file.” EX1001 57:10-24. Tajima teaches that in order to create the data fragments, a personal information dataset “is first divided into a plurality of data portions each of a predetermined fixed length, and this plurality of data

portions is then arranged as two [or more] data fragments, according to a set method of arranging.

A packet payload (as in Foster), however, is not created to protect the data. Rather it exists by virtue of the MPEG packetized elementary stream standard. EX1006 [0072]-[0073]; EX2014 (“An elementary stream is broken up into packets, forming a *packetized elementary stream* (PES).”). These packets allow for transmission of the content. See EX2015 626 (“**Packet** 1. Generic term for a bundle of data, usually in binary form, organized in a specific way *for transmission*.”); EX2016 257 (“a group of binary digits forming a message. The group is *transmitted* together”).

EX2033 ¶¶69-70.

In sum, Petitioner fails to demonstrate, that Tajima discloses attaching an encryption key to a packet, or that what Foster attaches its keys to is a data fragment. As a result, the Petition fails to explain why a POSITA would consider, much less be motivated to apply, Foster’s disclosures about encrypting the keys used to encrypt the packets of an MPEG video stream for transmission, to information regarding the keys (not the keys themselves) used to secure Tajima’s data fragments for storage. Nor does it explain why a POSITA would have any reasonable expectation that such a combination would be successful. As Dr. Rubin explained,

The silence of Tajima, on the one hand, about attaching the keys themselves to data fragments, and the lack of disclosure in Foster about

anything corresponding to a data fragment, means that a POSITA would not be motivated to combine (and would not have any reasonable expectation that) these references could be successfully combined to achieve the inventions disclosed in independent claims 1 and 9.

EX2033 ¶73. *See Dish Network LLC v. Entropic Comm's*, IPR2024-00560, Paper 11 (P.T.A.B. August 15, 2024) (in denying institution, the Board rejected a proposed obviousness combination based on “combining two fundamentally different systems for no reason other than that the modification or combination would allegedly meet the claims”).

(ii) Combining Tajima and Foster Renders the Key-Securing Method of Tajima Redundant.

A POSITA would not be motivated to combine Foster to Tajima for an additional reason: Tajima’s key information is already secured by hiding it—by attaching it to a data fragment it cannot decrypt, and storing the different data fragment/key information combinations in different locations. *See, e.g.*, EX1005 at [0110]-[1015]. Petitioner acknowledges this, stating that “Tajima-Foster [] obfuscates keys by attaching key information to a different data fragment...**and additionally obfuscates [Tajima’s] keys** by “encrypting [them] with a KEK [key encryption key]” according to the method of Foster. Pet., 41-42. Applying Foster to secure the key information through encryption would render the method already

used by Tajima to secure that information redundant. Neither Tajima nor Foster suggests that Tajima's method fails to provide adequate security, and Foster's method intimately tied to the need to transfer the title key used to encrypt the packets simultaneously with the packets themselves—a concern that is not present in Tajima.

As Dr. Rubin explains:

Foster acknowledges that its “title key is encrypted with the key encrypting key” precisely so that it “can then be transmitted along with the encrypted content.” EX1006, [0053]. By this suggestion, Foster ties the benefits of its KEK method to the need to secure the keys that encrypt the packets themselves (by encryption with a KEK) so that the keys can be transmitted together with the packets. If the packet encryption keys were not themselves encrypted, they could not be transmitted with the packets, as an attacker with access to the transmission would get both an encrypted packet and an unsecured key that can be used to immediately decrypt it. Tajima, in contrast, has no need to further secure its key information by encryption because it already secures that information by hiding it with a data fragment it cannot decrypt. Thus, an attacker with access to a system that stores fragments according to Tajima does not have the key information needed to decrypt that fragment.

EX2033 ¶75.

As a matter of law, it is not obvious to modify a reference that already achieves the benefit supposedly served by the proposed modification. *See, e.g., In re NTP*,

Inc., 654 F.3d 1279, 1299 (Fed. Cir. 2011) (finding claims not obvious because “the [prior art] already discloses an RF network that connects portable computers to the system. Thus, adding an RF network [as required by the claims] would render the prior art RF network superfluous.”); *Apple Inc. v. Cellular Comm’ns Equipment, LLC*, IPR2015-00576, Paper 7, 12 (June 12, 2015) (denying institution where “Petitioner...fails to provide a specific explanation why [the primary reference] did not already accomplish [the asserted benefits] by itself.”); *F5 Networks, Inc. v. Radware, Ltd.*, IPR2017-00124, Paper 48, 64-65 (Apr. 23, 2018) (no motivation for modification that “serve[s] no purpose”).

(b) *Foster Discourages Petitioner’s Proposed Combination.*

Even if one assumed, contrary to their disclosures, *see supra* Section II, that (1) the “key information” of Tajima includes the keys used to encrypt its data fragments; and (2) that MPEG packet payloads/content units of Foster correspond to a data fragment, a POSITA still would not be motivated to combine them. Any combination would require eliminating the benefits of both systems to create a system that cannot achieve the objective of either. Indeed, Foster discourages a POSITA from adopting the method of Tajima, by emphasizing the efficiency of keeping an encryption key and the packet it can decrypt together, and decrying the disadvantages of attaching an encryption key to a packet it cannot decrypt.

As shown above, *see supra* Section III.A.1, Tajima and Foster have fundamentally different objectives and modes of operation. Dr. Rubin explains:

In the embodiments of Tajima on which Petitioner relies, depicted in Tajima’s Figures 12 and 13, a dataset is divided into two fragments, X and Y”; each fragment is encrypted using a different key.” *Id.* 18 (citing Tajima EX1005, [0111], [0113]. After data fragments X and Y are encrypted, “information regarding the key that was used for the encryption of data fragment Y is attached to encrypted data fragment X, and information regarding the key that was used in the encryption of data fragment X is attached to encrypted data fragment Y.” In other words, each chunk is attached to, and stored with, information about a key that is not the one used to encrypt it. Tajima EX1005, [0111]-[0114]. This means that by design Tajima’s system cannot perform synchronized transmission.

Foster, by contrast, discloses a system in which “[t]he encrypted title key [is] attached to the content packet and the header for synchronized transmission to, or storage by a receiver. *Id.*, [0008] In fact, attaching the key to content it can decrypt for synchronized transmission of the two together is essential to Foster’s system—it is “the whole invention,” as Dr. Bhattacharjee opined at his deposition. EX2034, 32:20-23.

EX2033 ¶¶77-78.

The Petition asserts that in its proposed Tajima/Foster combination each title key would be attached to a different data fragment than the one it can decrypt, as is done with the key information in Tajima. Pet., 33-34. But doing that would entirely abandon what Petitioner's expert, Dr. Bhattacharjee, agrees is Foster's "whole invention"—the synchronicity between a packet and the key that can decrypt it. Foster discourages a POSITA from adopting a mode of operation that separates a key and the data it can decrypt.

Where, as a result of reviewing a reference, a POSITA "would be led in a direction divergent from the path taken" from that claimed in the patent, it "can preclude a determination" that the combination is obvious. *AstraZeneca AB v. Mylan Pharm. Inc.*, 19 F.4th 1325, 1337 (Fed. Cir. 2021). A POSITA cannot be motivated to combine references if one of them "criticize[s], discredit[s], or otherwise discourage[s] investigation" into the proposed combination. *Id.*; *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009). A POSITA reviewing Foster would understand that Foster discourages a POSITA from pursuing the combination proposed by Petitioner because it touts the advantages of keeping a key together with the data it can decrypt, and decries the disadvantages of the contrary path in which they are separated (as in Tajima). As Dr. Rubin explained:

Foster discloses that in prior art systems, encryption keys were separated from the content they encrypted. This created a problem because when the key and content are not synchronized by keeping them together, “the incorrect key might be used and the content could not be decrypted.” EX1006, [0007]. As explained in Foster’s specification, Foster’s invention solved this problem because “by transmitting the encrypted key as an integral part of the encrypted content, a receiver would receive the encrypted content as well as all information necessary to decrypt the content in a single stream.” *Id.*

EX2033 ¶81.

B. Petitioner Fails To Show A Motivation To Combine Tajima/Rivest (Ground 3; Claims 9-14).

Petitioner contends a POSITA would combine Tajima and Rivest because they “would have recognized the benefit of applying Rivest’s ‘all-or-nothing’ transforms (AoNT) to Tajima’s key information to protect Tajima’s plaintext keys without needing to maintain secret keys.” Pet., 46. According to the Petition, “Tajima-Rivest applies Rivest’s AoNT using the user’s public key provided to Tajima’s service sites...and thus beneficially avoids using secret keys.” *Id.* at 47.

A POSITA would not be motivated to apply “Rivest’s AoNT using the user’s public key” as Petitioner and its expert suggest. As Dr. Rubin explains,

Rivest says nothing about the use of public keys and is not designed to be used with public keys. Rivest is generally used in connection with symmetric encryption systems that require a secret key. Public key

encryption systems generally use different types of transformations. Instead of a public key, Rivest requires the use of a random number as the basis for its AoNT transformation. See EX1034 [Rivest], 213-14.

EX2033 ¶84.

Petitioner's proffered motivation should also be rejected because it is contradicted by Rivest itself. Rivest explains that the AoNT standing alone does not require the use of a secret key only because, standing alone, it does not "protect" anything. EX1034, 212. Rather, the AoNT adds additional protection to a data set that is otherwise separately encrypted or secured. *Id.* Because Tajima does not separately encrypt or parse its key information into smaller pieces, a POSITA would not see any benefit in combining it with Rivest. Per Dr. Rubin,

Rivest discloses that the AoNT is merely a "pre-processing" step "that has certain interesting properties," but by itself does not provide adequate protection to a dataset (such as the key information of Tajima). 1034 [Rivest] 212. Specifically, applying the AoNT to a dataset before it is further encrypted or divided into pieces forces an attacker to "decrypt the entire data set before [it] can determine" even one piece of the data set. *Id.*, 210. For example, AoNT is appropriate if one desires to require that a party in a transaction obtain all of the ciphertext before performing a decryption. However, if the data set has merely been transformed using the AoNT, without further encryption or splitting, "anyone" who knows the random number on which the

transformation is based can “invert” it to obtain the original dataset. *Id.*, 212. In the Tajima-Rivest combination proposed in the Petition, that number would be a public key that is known to anyone. Because Tajima does not suggest separately encrypting or parsing its title keys into smaller pieces, in my opinion, a POSITA would not see any benefit in combining it with Rivest’s AoNT based on a public key.

EX2033 ¶86.

Thus, Rivest’s AoNT cannot alone “protect Tajima’s plaintext [title] keys without needing to maintain secret keys.” *See* Pet., 46. Either further encryption of the transformed titled keys would be necessary—which **would require the system to maintain additional secret keys**, obviating Petitioner’s purported motivation—or the key would have to be fragmented into separately stored pieces, which would add further complexity to the system. *See* EX1001, 77:5-47. As Dr. Rubin explains:

In my opinion, Petitioner is simply wrong in contending that a POSITA would be motivated to combine Tajima with Rivest “to secure the plaintext keys without the need to maintain secret keys.” The AoNT transformation of Rivest cannot secure a key without a further encryption step or fragmentation step that would have to be added to Tajima. *See* EX1001, 77:5-47. If further encryption is used, that would require the system to use and maintain another secret key. Fragmenting the key and storing the pieces in different locations would be another way of securing the transformed title key, but that also is a step that

would have to be added to Tajima that would require maintaining information about the locations of the pieces of the fragmented key.

E2033 ¶87.

Petitioner additionally ignores the substantial drawback associated with using AoNT. As Dr. Rubin explains:

Rivest also points out that “all-or-nothing encryption has **terrible** error-propagation properties” because if any pseudo-message block is damaged “then it is likely that **every** message block will be damaged.” EX1034, 216. Accordingly, redundancy information should be included in any data set before it is transformed using the AoNT, a practice that is suggested in the ’116 (see 77:23-36) but which would have to be added to Tajima.

Tajima is directed to a database for user information. Far from suggesting the use of redundant information, Tajima states that, as to its data fragments, no one fragment is sufficient to recreate the data set. EX1006. Introducing redundancies into such a database could also tax storage space and could slow the processing of user data to the extent required to remove redundant information to efficiently transmit and use the data.

EX2033 ¶88-89.

C. Petitioner Fails To Show A Motivation To Combine Tajima/Rivest/Shyu (Ground 4; Claims 1-3, 6).

Petitioner proposes combining Shyu with Tajima/Rivest (Pet., 48-50), but never clearly explains why adding Shyu is required for claims 1-3, 6. Petitioner suggests that Shyu provides the “metadata” required to meet Petitioner’s construction of the phrase “data indicative of at least one of the plurality of different encryption keys.” *Id.* at 50.

Shyu discloses “a data encryption method and system for effectively guarding against piracy of source data during data transmission.” EX1016, 1:32-34. Shyu explains that “the object of the present invention is to provide a method and system for dynamic data encryption,” in which the encryption algorithm is “dynamically changed to guard against piracy when data is transferred between two entities, such as a transmitter and a receiver of a data processing system.” *Id.*, 1:35-41.

Petitioner contends a POSITA “would have recognized the benefit of applying different encryption algorithms to different data fragments as taught by Shyu to avoid known security risks of using a fixed encryption algorithm.” Pet., 48. Petitioner is wrong.

First, **no** POSITA would be motivated believe security would be improved by applying of different encryption algorithms to different pieces of the same data set

(per Shyu) because doing so would violate Kerckhoff's Principle, a long-standing and fundamental tenet of cryptography. As Dr. Rubin explains,

Kerckhoff's Principle...is one of the foundational rules of cryptography.... [T]he rule states that "[t]he cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience." EX2007, 3. In other words, it holds that holds that a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge. *Id.* Stated differently, Kerckhoff's principle demands that security rely solely on the secrecy of the key. Kerckhoff's Principle has been widely embraced by cryptographers for decades. This stands in stark contrast to their rejection of the notion of "security by obscurity" which is the idea that higher security can be achieved by keeping a cryptographic algorithm obscure (or hidden) from public view. *Id.* There are a number of reasons for Kerckhoff's rule, including that: (1) it is easier to secure a random key than a random algorithm; (2) the number of good encryption algorithms is limited and it is not difficult for an attacker to try all of them; (3) it ensures that the level of security provided by an encryption system can be mathematically proven, whereas the likelihood that the method behind an *ad hoc* system such as Shyu might be leaked or disclosed cannot be reliably estimated.

EX2033 ¶94.

Shyu's anti-piracy system is a prototypical attempt to achieve security through obscurity, to the extent it proposes to conceal or obscure the encryption algorithms

(Pet., 48-49) used on any data set or piece of a data set. Because it violates Kerckhoff's principle, an POSITA would be discouraged from following the path it discloses, much less motivated to combine it with Tajima and Rivest.

Moreover, adding dynamic encryption as taught by Shyu provides no benefit to Tajima's system, and adds substantial complexity. The purported goal of Shyu is to protect against software piracy "**during**" transmission of the software from a transmitter to a receiver. *Id.*, 1:5-10. As Dr. Rubin explained:

Shyu seeks to address the problem of piracy by an attacker during the transmission of a data set in blocks ***from a single source to a single destination***. In those circumstances, an attacker watching the transmission has access to all of the transmitted blocks. If the same encryption algorithm is used for every block, an attacker with access to the transmission only has to correctly ascertain the algorithm once, and can could use that knowledge to decrypt the rest of the entire transmission. But Tajima does not present this risk, because in Tajima ***different pieces of the personal information data set are transmitted to different destinations***. There is no logical reason to dynamically change the encryption method for different data fragments, because a single attacker is unlikely to have access to all of the fragments that comprise the data set.

EX2033 ¶98. Combining Shyu with Tajima and Rivest would add the substantial complexity associated with maintaining multiple encryption algorithms and tracking

encryption algorithm “metadata,” without providing any substantial security benefits.

D. Petitioner’s Tajima Combinations Are Hindsight-Driven And Do Not Consider Their Drawbacks.

“The Board must weigh the benefits and drawbacks of the modification against each other, to determine whether there would be a motivation to combine.” *Arctic Cat Inc. v. Polaris Indus.*, 795 Fed. App’x. 827, 833 (Fed. Cir. 2019); *Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000); *Koninklijke Philips N.V. v. Quectel Wireless Sols. Co.*, No. 2023-1223, 2024 WL 3665345, at *2–3 (Fed. Cir. Aug. 6, 2024) (substantial evidence of motivation to combine where PTAB considered expert testimony that discussing how a POSITA would weigh benefits and drawbacks of the combination); *Intel Corp. v. Qualcomm Incorp.*, 21 F.4th 784, 796 (Fed. Cir. 2021); *Everstar Merch. Co. v. Willis Elec. Co.*, No. 2021-1882, 2022 WL 1089909, at *4 (Fed. Cir. Apr. 12, 2022). The Petition fails to consider the drawbacks of *any* of its proposed Tajima combinations (Tajima/Foster, Tajima/Revist, or Tajima/Rivest/Shyu) and its proposed obviousness combinations should be rejected for that reason alone.

Petitioner’s purported motivations to combine Tajima with Foster or Rivest alone or with Rivest and Shyu together should also be rejected because they are

entirely hindsight-driven, using the '116's claims and teachings as a roadmap. As

Dr. Rubin explains:

It is my opinion that a POSITA would not have recognized any of Petitioner and Dr. Bhattacharjee's proposed motivations to combine Tajima with Foster, or Rivest or Rivest/Shyu at the time of the '116 alone or with Rivest and Shyu. Dr. Bhattacharjee's motivations to combine Tajima with Foster, Rivest or Rivest/Shyu seem entirely driven by what the claims require. Dr. Bhattacharjee first argues that it would be "obvious" to modify Tajima such that the "key information"—which, as I previously explained, does not indicate the explicit inclusion of the encryption key—now includes the encryption key itself. EX1003 ¶102; Pet., 22. Later, however, Petitioner argues that Tajima's (now-modified) teaching of attaching keys to the encrypted data chunks is flawed, making Tajima's system less secure which would, supposedly, motivate a POSITA to turn to Foster or Rivest to provide methods of securing those attached keys. *Id.* ¶¶141-59, 184-92. This is creating a problem in order to provide a solution that would satisfy the claims. No such security flaw existed in Tajima before Petitioner's Dr. Bhattacharjee's proposed modification of including the encryption keys with the key information. Indeed, applying a key-encryption key or AoNT to "information regarding the key" would do little to improve security. Adopting the solution of "transforming" the keys is a solution seems only driven by Dr. Bhattacharjee's Petitioner's proposed modification which created the

problem in the first place, not any preexisting technological need or benefit derived from improving upon Tajima's unaltered teachings.

EX2033 ¶101.

In addition, the Petition implicitly acknowledges that its proposed Rivest combinations (Grounds 3 and 4) are hindsight-driven when it admits that it is using the '116's teaching of using AoNT on encryption keys to supply the motivation to combine Tajima and Rivest. The Petition states that

The '116 patent itself acknowledges that AoNT was "well-known" and that "it *will* be understood that the AoNT may be applied to encryption keys used to encrypt the data portions following parsing and splitting."

EX1001, 77:13-43; Bhattacharjee, ¶184.

Pet., 47.

Finally, consistent with the hindsight driven nature of its other obviousness grounds, Petitioner seems to have included Shyu, not because a POSITA would be motivated to combine it with Tajima and Rivest, but in a result-driven effort to meet a claim limitation under one of the parties' propose claim constructions.

Ultimately, Petitioner's proffered modifications provide little, if any, benefit to Tajima's system and are the result of precisely the sort of hindsight-driven analysis the Federal Circuit has rejected. As the Federal Circuit has held, "[t]he inventor's own path itself never leads to a conclusion of obviousness; that is hindsight." *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 165 (Fed.

Cir. 2021) (quoting *Otsuka Pharm. Co., v. Sandoz, Inc.*, 678 F.3d 1280, 1296 (Fed. Cir. 2012)); *InTouch Techs., Inc. v. VGo Commc 'ns., Inc.*, 751 F.3d 1327, 1351 (Fed. Cir. 2014) (rejecting expert's obviousness theory that "relied on the [] patent itself as her roadmap for putting what she referred to as pieces of a 'jigsaw puzzle' together."); *In re Conrad*, 759 Fed. App'x. 982, 985–86 (Fed. Cir. 2019) (obviousness requires "a specific" rationale to combine limitations to make the claimed invention that is "unrelated to the rationale behind the inventor's reasons for making the [claimed] invention.") (collecting cases); *Ruiz v. A.B. Chance Co.*, 357 F.3d 1270, 1275 (Fed. Cir. 2004) ("This form of hindsight reasoning, using the invention as a roadmap to find its prior art components, would discount the value of combining various existing features or principles in a new way to achieve a new result—often the very definition of invention").

IV. THE FOSTER-HAYHURST GROUND FAILS (GROUND 5, CLAIMS 1-2, 5, 9 AND 11).

Petitioner's Foster/Hayhurst combination fails because Petitioner fails to prove that Hayhurst is analogous art or that a POSITA would be motivated to combine Foster/Hayhurst as proposed.

A. Petitioner Fails To Demonstrate That Hayhurst Is Analogous Art.

The Foster/Hayhurst ground fails because Petitioner fails to prove Hayhurst is analogous art to the '116 Patent. "A reference qualifies as prior art for an

obviousness determination...only when it is analogous to the claimed invention.” *In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011). An obviousness ground that relies upon non-analogous art fails, because a POSITA would have no reason to consider the non-analogous art, much less a motivation to combine it with another reference. *Id.*, 1352. Petitioner bears the burden of demonstrating a reference is analogous. *Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1377 (Fed. Cir. 2023).

To be analogous, a reference must be either (1) from the same field of endeavor as the patent-at-issue, or (2) reasonably pertinent to the particular problem with which the inventor of the challenged patent is involved. *In re Clay*, 966 F.2d 656, 658-59 (Fed. Cir. 1992).

1. Hayhurst And The '116 Patent Do Not Share The Same Field Of Endeavor.

Petitioner makes no attempt to show that Hayhurst and the '116 share the same field of endeavor. Nor could it. As Petitioner and Dr. Bhattacharjee admit, the '116's field is securing data while Hayhurst's is decentralized electronic media delivery. EX1007, 13 (recognizing that “‘one aspect of the present invention’ is a method for securing data from unauthorized access or use.”); EX1003 ¶ 31 (same); Institution Decision 2-3; Pet., 55 (“Hayhurst concerns ‘**electronic media delivery, such as video-on-demand**’”); EX1003 ¶ 228 (same); EX2034 101:19-25.

To discern the field of endeavor, the Federal Circuit has looked to various sources, including a patent’s title, claim preamble, abstract, “background of invention” and “field of the invention,” and the function and structure of the claimed inventions. *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1380-81 (Fed. Cir. 2019) (determining field from title, claim preamble); *Kamstrup A/S v. Axioma Metering UAB*, 43 F.4th 1374, 1384 (Fed. Cir. 2022) (discerning field by comparing abstracts); *In re Bigio*, 381 F.3d 1320, 1326 (Fed. Cir. 2004) (“The Board...correctly set the field...by consulting the structure and function of the claimed invention”); *In re Wood*, 599 F.2d 1032, 1036 (CCPA 1979) (field from “Background of Invention”); *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1237-38 (Fed. Cir. 2010) (similar); *Airbus*, 941 F.3d at 1381 n.8 (“[T]he specification of each reference includes a ‘Field of the Invention’ section that distinctly describes each applicable field of endeavor.”).

Here, as Dr. Rubin explains:

Each of these traditional sources for identifying a field of endeavor uniformly confirm that the ’116’s field is securing data.

The ’116’s Field Is “Securing Data”	
Title	“ secure data parser method and system”
Abstract	“ secure data parser for “ securely storing and communicating data ”
Field of Invention	“ securing data from unauthorized access or use.” EX1001, 1:21-22.

Background of the Invention	focuses on the need “for ensuring data stored and transmitted... cannot be read or otherwise compromised ” and seeks “to provide a cryptographic system whose security is user-independent... ” <i>Id.</i> , 1:31-33, 2:36-37.
Summary of the Invention	“one aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use.” <i>Id.</i> , 2:39-41.
Claims	each claim concerns “securely storing a data set” or “securing a data set”

Hayhurst does not share this field. Hayhurst’s field, per these same traditional sources, is “decentralized media delivery.”

Hayhurst’s Field Is “Decentralized Media Delivery”	
Title	“Decentralized Media Delivery”
Abstract	“A decentralized approach to delivering a media file...”
Technical Field	“This application relates to the field of electronic media delivery...” EX1007, [0002].
Background of the Invention	Focuses entirely upon delivering movie files. <i>Id.</i> , [0003]-[0004].
Summary of the Invention	“The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files. ” <i>Id.</i> , [0005].
Specification/Figures	“FIG. 1 is a block diagram of a system adapted for carrying out the decentralized media delivery of the present invention.” <i>Id.</i> , [0012]

	“FIG. 4 is a flow diagram showing how the <i>decentralized media file delivery</i> of the present invention is carried out.” [0015]
Claims	each claim concerns “securely storing a data set” or “securing a data set”

EX2033 ¶¶107-108.

While Hayhurst includes some disclosures about the security of the media files to which it is directed, Federal Circuit precedent confirms that art is not analogous merely because it includes disclosures that tangentially relate to the field of the patent at issue. Indeed, even art that is in the same general technological area as the subject patent may not be in the same field of endeavor. While Hayhurst mentions security, that is not Hayhurst’s field of endeavor (as established by the traditional sources discussed above). Hayhurst does not teach, for example, that

prior art systems did not adequately secure media files, or that its invention addresses address a need for more security. EX1007 [0003]-[0005]; EX2033 ¶110.³

Hayhurst's field is decentralized delivery of media files. That it also mentions the "secure handling and storage" of these files, does not alter or expand its field to encompass the "securing data" field of the '116.

³ In *Clay*, for example, the patent-at-issue and the allegedly analogous art (Sydansk) were two patents owned by the same company (Marathon Oil), both references related to gels used in the oil industry, and the district court noted that the gels were "similar" in some ways. *Clay*, 966 F.2d at 657-60. But the Federal Circuit found that the Board clearly erred in finding Sydansk analogous because the patent-in-question's "field of endeavor is the *storage* of refined liquid hydrocarbons" whereas "[t]he field of endeavor of Sydansk's invention...is the *extraction* of crude petroleum." *Id.*, 659 (italicization in original); see also *Wang Labs., Inc. v. Toshiba Corp.*, 993 F.2d 858, 864-65 (Fed. Cir. 1993) (reference not analogous to subject patents merely because claimed subject matter of both "relates to memories," where the reference "involves memory circuits in which modules of varying sizes may be added or replaced" while "the subject patents teach compact modular memories").

2. Hayhurst Is Not Reasonably Pertinent to the Problem the Inventors of the '116 Patent Were Addressing.

The Federal Circuit has made clear that “the purposes of both the invention and the prior art are important in determining whether the reference is reasonably pertinent to the problem the invention attempts to solve.” *Clay*, 966 F.2d at 659. Thus, “when addressing whether a reference is analogous art with respect to a claimed invention under a reasonable-pertinence theory, the problems to which both relate must be identified and compared.” *Donner Tech., LLC v. Pro Stage Gear, LLC*, 979 F.3d 1353, 1359 (Fed. Cir. 2020). If the reference “is directed to a different purpose, the inventor would accordingly have had less motivation or occasion to consider it.”

Here, Petitioner cannot meet its burden of establishing that Hayhurst is analogous because the Petition does not identify the problems to which Hayhurst or the '116, respectively, are directed, let alone compare those problems. A comparison establishes that Hayhurst is not reasonably pertinent to the problem the '116's inventors were trying to solve, including the need “to provide a cryptographic system whose security is user-independent while still supporting mobile users.” EX1001, 2:6-8. As Dr. Rubin explains:

A comparison establishes that Hayhurst is not reasonably pertinent to the problem the '116's inventors were trying to solve. The '116 is

directed towards creating a cryptographic system whose security is user independent, while still supporting mobile users. EX1001, 2:36-38. The '116 is directed towards the “ever-increasing need ... for ensuring data stored and transmitted” to not “be read or otherwise compromised.” *Id.*, 1:31-40. The '116 discusses certain prior art methods of securing data and the ways in which those methods may be compromised because they rely upon users. *Id.*, 1:34-40 (deficiencies in login/password systems); 1:54-2:07 (deficiencies in public-key systems that are “highly reliant on the user for security”), 2:20-32 (deficiencies in biometric systems that “suffer[] from a variety of drawbacks” from user losing/breaking smartcard). Consequently, the '116 addresses the need “to provide a cryptographic system whose security is user-independent while still supporting mobile users.” EX1001, 2:26-38.

EX2033 ¶112.

Hayhurst, in contrast, is directed towards “address[ing] the prohibitive bandwidth requirements for a content provider associated with delivering video-on-demand or other large media files.” EX1007 [0003, 0005]. Hayhurst explains that

[i]t is usually not economically feasible for the operator of, for example, a cable television (CATV) system (or other content provider) to provide for delivery-on-demand a large number of movie selections to subscribers ***because such a system requires an extensive amount of bandwidth between the content provider and each of the subscriber units*** (televisions or other display devices) of the network.

Id., [0004]. In order to solve this problem, Hayhurst teaches “a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units.” *Id.*; EX2033 ¶114. In his declaration and at his deposition, Dr. Bhattacharjee agreed that Hayhurst is directed towards the “problem” of extensive bandwidth associated with providing “delivery-on-demand” media content. EX1003 ¶ 178; EX2034, 87:7-13; 92:1-11.

Hayhurst and the ’116 are directed towards addressing entirely different problems. As Dr. Rubin explains:

The ’116, again, addresses eliminating user vulnerabilities in storing sensitive information. Hayhurst, by contrast, addresses the prohibitive bandwidth requirements for video-on-demand from the perspective of the content provider. EX1007, [0003]-[0005].

Security is merely an ancillary benefit to Hayhurst’s solution of decentralizing content delivery. And, what little Hayhurst has to say about encryption does not suggest that it is directed towards securing data in a manner that is “user-independent.” Rather, in Hayhurst’s system, a subscriber requests both an encrypted movie and an encryption key. EX1007, [0028], [0030]. While the movie is originally dispersed amongst thousands of subscribers, it is reassembled, along with the key, by a single user. Thus, the security of the data (the movie) is user-dependent.

EX2033 ¶115-16.

Thus, Hayhurst is not reasonably pertinent to the '116 because a POSITA would not have expected to solve a problem with securing data sets in general by considering a reference directed to reducing the bandwidth required to transmit video-on-demand. Hayhurst's tangential remarks regarding the security of media files do not change this analysis. *See, e.g., Clay*, 966 F.2d at 660, 658-59 (district court finding of reasonable pertinence was "clearly erroneous" where a POSITA "would not reasonably have expected to solve the problem of dead volume in tanks for storing refined petroleum by considering a reference dealing with plugging underground formation anomalies."); *Wang*, 993 F.2d at 864 (prior art memory modules not reasonably pertinent to patented memory modules); *Polygroup Ltd. v. Willis Elec. Co., Ltd.*, IPR2016-01610, Paper 187, 31, 35-40 (Feb. 26, 2018) (reference not reasonably pertinent despite including "structurally and functionally similar" electrical connectors).

In sum, Petitioner's second ground fails because the Petition fails to establish that Hayhurst is analogous art under either the "same field of endeavor" or "same problem" tests.

B. Petitioner Fails To Demonstrate That A POSITA Would Be Motivated To Combine Foster And Hayhurst.

A POSITA would not be motivated to combine Foster and Hayhurst because they are incompatible and have conflicting goals. Foster is directed towards real-

time streaming of television and live events; as such, it is concerned with avoiding delays that interfere with immediate access to content (*e.g.*, when a user changes a channel). *See supra* III.A.1. Hayhurst, by contrast, is directed to reducing the bandwidth required by a content provider in a video-on-demand context, where immediate access is unnecessary and, in fact, impossible. Hayhurst's method shifts the bandwidth burden from the content provider but does so in a fashion that introduces, rather than avoids, delays. A POSITA would not be motivated to combine Hayhurst's decentralized content storage into Foster because doing so would frustrate Foster's goal of avoiding delays, render Foster unsuitable for streaming live television, and make Foster's system less secure. Fundamentally, Petitioner's combination would make Foster's system worse for no discernible benefit.

1. Foster Provides Synchronized Transmission To Avoid Delays.

As discussed above, Foster's system is directed towards synchronizing the transmission of encrypted content packets with the keys used to encrypt those packets, so that each packet can be viewed as soon as it is received. *See supra* II.A.1. This fundamental goal is reflected in Foster's title, abstract, field of the invention, background of the invention, summary of the invention, and its disclosure generally. EX1006, Title; Abstract, [0002], [0008]. Both experts agree that Foster is directed

towards the synchronized transmission of encrypted content with corresponding encryption keys, EX2033; EX2034, 16:8-12, and at his deposition Dr. Bhattacharjee testified that “synchronous transmission to a receiver [to] foster random access to content” was “the whole invention in Foster,” EX2034, 32:20-23.

Foster’s synchronization is directed towards reducing delays in viewer access to content as it is transmitted by a provider. Per Dr. Rubin:

Foster seeks to improve upon prior art systems that were susceptible to “loss of synchronization between the content and the keys.” *Id.*, [0006]. The lack of synchronization impacted user experience with “inherent latencies” and “delays,” particularly when “providing random access of protected content,” *e.g.*, when the user changes the channel and when the image the new image displays. *Id.*, [0006], [0052] (“because delivery of keys and protected content are non-synchronized in a CAS, certain latencies such as delays are inherent in attempting to gain random access to the content.”); [0056] (without synchronization, “a delay could be incurred between when encrypted content is received and when it [is] accessed (*e.g.*, between when a channel is changed and when an image is displayed).”); [0063] (similar); [0064] (“both DRMS and CAS have inherent latencies (*e.g.*, delays) in providing random access [to] content.”). Foster, moreover, indicates that “synchronous transmission to...a receiver fosters random access to the content.” *Id.*, [0007]; [0052].

EX2033, ¶120.

As discussed above, *see supra* Section III.A.1.i, Foster processes content into “content unit[s]” consisting of an encrypted content packet and the “title key” used to encrypt the packet. The title key is itself encrypted with a “key-encrypting-key,” or “KEK,” before it is combined with the content packet in a single content unit. EX1006, [0008]. As illustrated in Figure 16 below—which Petitioner consistently relies upon (Pet., 53, 65)—Foster’s system transmits content units **directly** to **recipient 430** on a one-to-one basis:

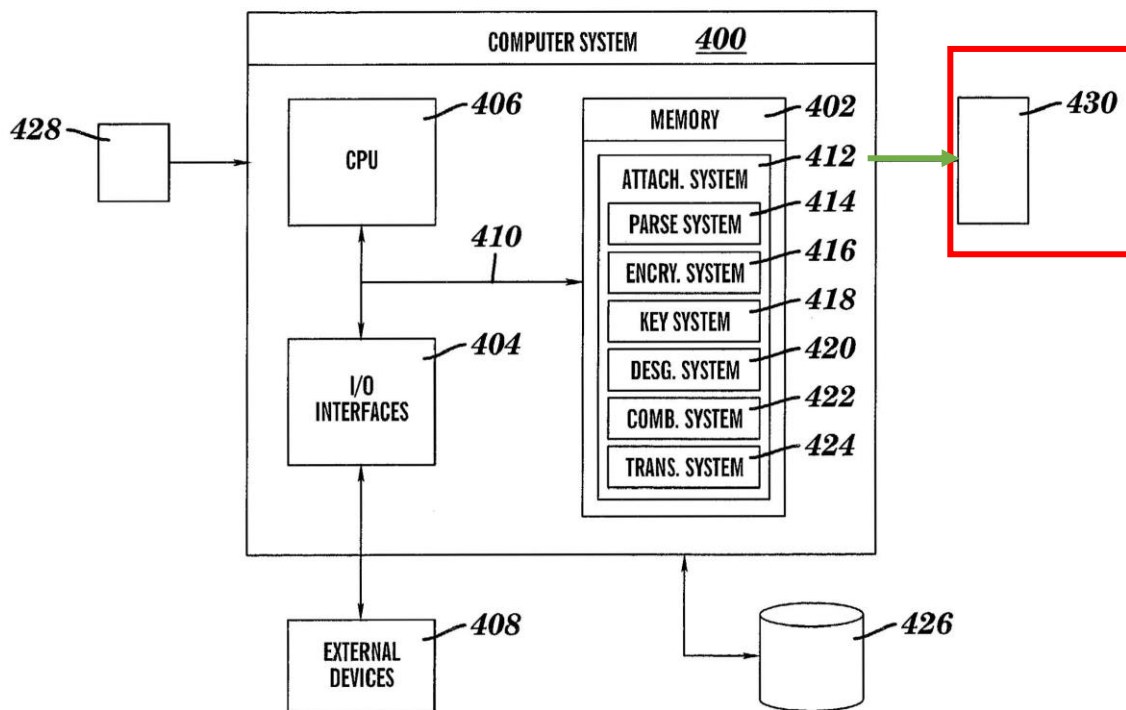


FIG. 16

EX1006 Fig. 16; [0078] (“computer system 400...process[es] content units of an elementary content stream received from source 428, and transmit[s] the processed content units to a recipient 430.”). Because each content unit contains both the content and the key, each content unit may be encrypted and transmitted by the source as it is generated, and then decrypted and viewed without delay. *Id.*, [0064]; EX2033, ¶121.

Foster seeks to improve on prior art cable television systems and teaches that its system processes and transmits content units between a “[c]ontent [s]ervice [p]rovider” “such as a cable service provider” (EX1006, [0039]) and a “[r]eceiver” “such as a set-top box” (EX1006, [0040]). See also *id.*, Fig. 16, [0006] [0052], [0078]. Consequently, as Dr. Rubin explains, Foster’s innovations are primarily useful in a streaming context where the individual content units are the serial packet components of a real-time content stream:

Foster’s teachings of synchronized transmission are particularly significant in a streaming context contemplated by Foster’s Figure 8, which Petitioner relies upon (*e.g.*, Pet., 56, 65-66). “In streaming, multimedia data is transferred in a stream of packets that are interpreted and rendered in real time by a software application, as the packets arrive in the user’s terminal.” EX2035, 220. Because packets are transmitted as a stream and rendered in real-time, any delays have an especially noticeable impact. When watching, *e.g.*, a live sporting event, any

delay in receiving, decrypting and/or rendering each content unit in a stream would be a significant drawback. Figure 8 depicts the “Encryption of [an] Elementary Stream,” provided to a set-top box which has “random access points (points in stream where player can start [displaying the stream])”:

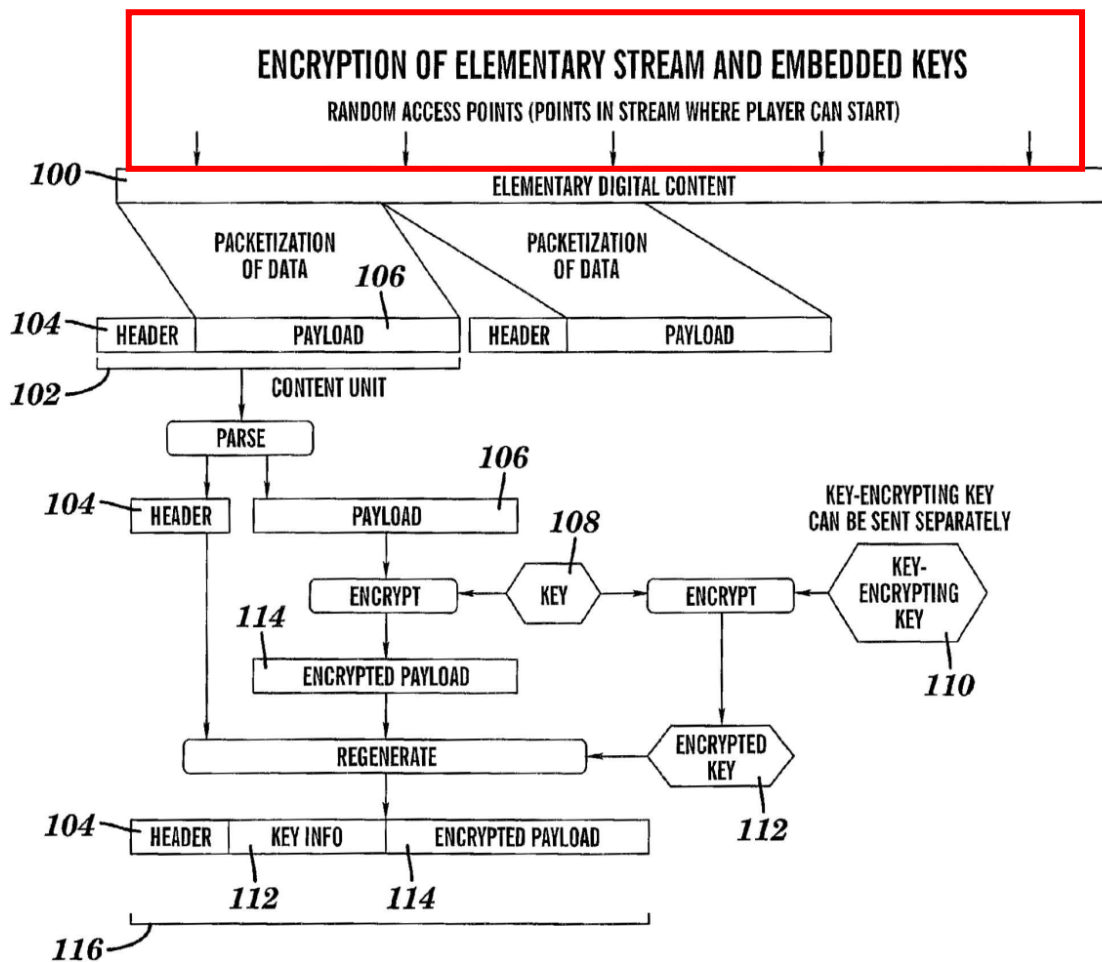


FIG. 8

EX2033 ¶122 (citing EX1006 Fig. 8). Foster makes clear that when content and keys are not sent synchronously, the type of random access of content contemplated by Figure 8 “is not possible” in the streaming context. *Id.*, [0063]; *see also* [0064], [0071].

2. Hayhurst’s Goal Is Directed to Reducing the Bandwidth Requirements for the Provision of Content Where Immediate, Random Access Is Not Required.

Hayhurst, by contrast, is not concerned with synchronous transmission, avoiding delays, or facilitating real-time streaming in any way. Hayhurst purports to facilitate the transmission and playback of content **files**, not content **streams**. Specifically, Hayhurst aims to overcome “prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files” to a subscriber network. EX1007, [0005]. Hayhurst teaches that, in light of the size of these files and the bandwidth required to transmit them, it is “usually not economically feasible” for a content provider “to provide for delivery-on-demand [of] a large number of movie selections to subscribers.” *Id.*, [0004]; Section IV.A.2.

To address the bandwidth problem, Hayhurst “shifts the bandwidth requirements away from the content provider [] to the network of subscriber units.” EX1007 [0005]. As Dr. Rubin explains:

Hayhurst divides a movie file into segments that are then stored across a network of subscriber units. When a movie is requested by one

subscriber, the system directs other subscribers to send their respective segments of the file to the requesting subscriber. When all of the segments are received at the requester's computer, they are then decrypted and the file is reassembled from the collection of segments for viewing. EX1007 [0006]. Hayhurst's system is a network of "thousands of subscribers." *Id.*, [0016]; EX2034 101:15-25.

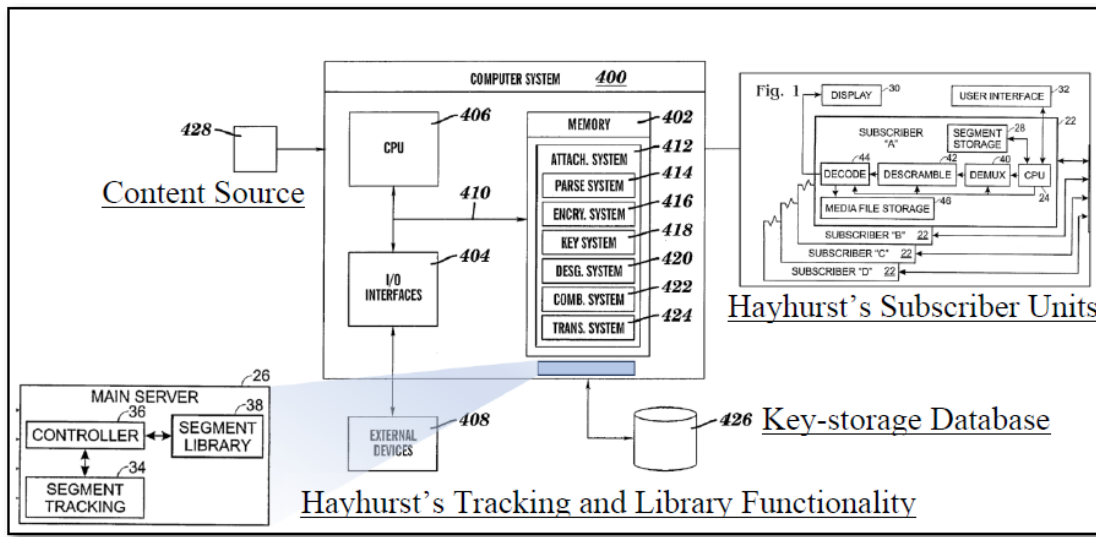
Hayhurst's system is not compatible with real-time streaming or random-access viewing of live television. Hayhurst requires that an entire movie file be segmented, and the segments transmitted to, and stored among, the members of a subscriber network before the movie can even be requested for viewing by any individual subscriber. Beyond that, because the segments are not stored in or received in any particular order, the movie cannot be viewed at all by the individual subscriber until (i) **all** segments are received from the subscriber network by the subscriber, (ii) the requesting unit obtains authorization, and (iii) the packets are descrambled and then reassembled into the complete movie file. EX1007, [0029]; [0030]; EX2034, 101:19-25. Thus, Hayhurst's system requires all segments to be received and for the entire file to be reassembled the system can play the movie.

EX2033 ¶125-26. As others in the field have recognized, in "download and play," systems such as Hayhurst "the client has to download and store first ***the whole media content*** on his PC and only then he/she will be able to view and use it." EX2035, 219. This requirement "***exclud[es] the use [of such systems] for covering live***

events, as the multimedia information that is to be transmitted cannot be ‘a-priori’ available.” *Id.*

3. Petitioner’s Combination Involves Storing and Distributing All of Foster’s Content Units per Hayhurst’s Method.

Petitioner posits a combination of Foster and Hayhurst in which Foster’s media **content units** are transmitted and then stored in Hayhurst’s decentralized media **file** storage system. Specifically, “Foster’s encrypted content units” would be stored “on multiple storage devices...based on Hayhurst’s techniques” “for storing [and distributing] encrypted data segments” of a media file. Pet., 67, 63. In Petitioner’s “exemplary implementation of Foster-Hayhurst,” illustrated below, “Foster’s ‘computer system 400’ is augmented...to control distribution of, and access to, Foster’s encrypted content portions on [Hayhurst’s] ‘subscriber units.’” *Id.*, 65. Thus, in Petitioner’s combination, Foster’s “content stream 100” “is parceled into content units 102” (*id.*, 52) and rather than sending content units directly to the requesting subscriber, the content units would be distributed amongst Hayhurst’s network of thousands of subscribers.



Foster-Hayhurst (exemplary implementation)

Id., 64; 62 (“POSAs would have numerous reasons to adopt Hayhurst’s distributive storage technique in Foster’s system so that Foster’s encrypted content units for a media file would be distributively stored on different consumer devices...as Hayhurst teaches”); 63 (similar); 64 (similar). At his deposition, Dr. Bhattacharjee admitted that this “is the only implementation of the combination that is described or relied on in the Petition. EX2034, 126:3-9.

4. A POSITA Would Not Be Motivated To Combine Foster And Hayhurst As Proposed.

In evaluating a POSITA’s motivation to make a combination, “[t]he Board must weigh the benefits and drawbacks of the modification against each other, to determine whether there would be a motivation to combine.” *Arctic Cat Inc. v. Polaris Indus.*, 795 Fed. App’x. 827, 833 (Fed. Cir. 2019); *see also* Section III.D

(additional citations). Critically here, the Federal Circuit has held that, as a matter of law, a POSITA would not be motivated to render a reference “inoperable for its intended purpose” or to change its “principle of operation.” *Plas-Pak Indus. v. Sulzer Mixpac AG*, 600 Fed. App’x 755, 759 (Fed. Cir. 2015) (POSITA not motivated to make reference “inoperable for its intended purpose” and “a change in a reference’s ‘principle of operation’ is unlikely to motivate a person of ordinary skill to pursue a combination with that reference”); *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984); *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374 (Fed. Cir. 2007); *Tec Air, Inc. v. Denso Mfg. Mich., Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999); *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959) (not motivated to change reference’s principles of operation).

A POSITA would not be motivated to combine Foster and Hayhurst as Petitioner proposes because, far from providing any significant benefit, the proposed combination would thwart Foster’s goals, make Foster inoperable for its intended purpose, and compromise any security benefits otherwise provided by Foster alone.

Petitioner’s combination suffers from three critical flaws. *First*, the combination would introduce the specific delays Foster is designed to avoid, making the synchronization that is the primary purpose of Foster unnecessary. *Second*, the combination would not be capable of providing streaming (*e.g.*, real-time television) or random access to content, contravening Foster’s intended purpose. *Third*,

Petitioner's combination would reduce security as compared to Foster by exposing Foster's key-encryption keys. The Petition does not address any of these issues.

- (a) *Adding Hayhurst's Delivery Method to Foster's System Exacerbates the Underlying Problem Of Delay Foster Seeks to Solve.*

As explained above, in Foster's system, because each packet in an elementary content stream can be generated as the content is created, and then sent directly to the recipient with its title encryption key, each packet can be viewed without delay, allowing for immediate, random access to the content. *See supra* Sections III.A.1, III.B.1.

Replacing Foster's direct distribution of content streams with Hayhurst's decentralized delivery and storage of media files would introduce the delays it was Foster's goal sought to avoid. Hayhurst, again, concerns a decentralized delivery system where a movie file is divided up into segments stored amongst thousands of subscribers. By its logic, Hayhurst's system inherently requires significant delays before content can be played. *See supra* Section IV.B.2. As Dr. Rubin explains:

Petitioner's Foster/Hayhurst combination would result in inevitable, significant, and crippling delays, the very thing Foster was intended to avoid. Petitioner's proposed combination of Foster and Hayhurst relies upon Hayhurst's methods of storing and delivering segments of media files. Pet., 64. In Petitioner's proposed combination, all of Foster's encrypted content units would, rather than be sent directly to the

requestor as in Foster, instead be distributed across thousands of subscriber units before they are then, when requested, sent to a requesting unit, as taught in Hayhurst. EX1007, [0016].

This introduces delay in a number of ways. First, in Hayhurst the content must exist as a discrete file before it can be divided into segments and distributed for storage among the subscriber network. (This is in stark contrast to Foster, where the content units can be created and transmitted as the stream of content is generated.) Then, in Hayhurst, the main server, upon receiving a request, must direct the thousands of subscribers to send segments to the requestor. *Id.*, [0028] (“after the main server receives a movie request 104 from a requesting subscriber ..., the server responds 106 by sending over the network instructions to the network subscriber units to direct all of the segments of the requested movie to the requesting subscriber.”). Should there be one or more missing packets, which there inevitably would be for subscribers whose systems are turned off, internet is down, are no longer subscribers, etc., the main server must either direct another subscriber with the same packet to resend it or redistribute the packet. *See id.*, [0025] (“Each segment [] is copied and distributed to a plurality of different subscribers to provide for redundant availability of each segment in the event a subscriber’s segment storage 28 becomes inaccessible. As noted, the main server’s segment-tracking module 34 can ...facilitate replacement or redistribution of segments when necessary.”); EX2034, 106:17-109:6. Accordingly, the requesting unit must wait until “**all** packets are received” before sending a request to

the main server to decrypt the segments and reassemble the movie file. EX1007, [0029] (“The subscriber unit CPU 24 and associated buffers (not shown) log the received packets and, once ***all packets*** are received, sends a notice to the main server 26 that ***all packets*** now reside in the unit of the requesting subscriber.”). Only after all of the packets are on the requesting unit does the main server “transmit[] authorization.” *Id.*, [0029]. After obtaining authorization, the receiving unit may descramble, process, and reassemble the entire media file for playback. *Id.*, [0029]-[0030]; EX2034 109:8-111:1. Only after all of these steps are completed, the movie can be viewed.

Consequently, Hayhurst’s methods of storing and delivering content make playback delays—the underlying problem Foster seeks to address—exponentially worse. Rather than immediately streaming content in packets that are synchronized with the encryption keys as Foster does, Petitioner would have Foster’s system store and deliver content using Hayhurst’s decentralized, time-consuming method. In other words, Petitioner proposes changing Foster’s method which has been designed to reduce delays to one that prioritizes bandwidth at the expense of creating delays.

In my opinion, a POSITA would not be motivated to change Foster to implement methods which greatly exacerbate the underlying problem Foster seeks to address.

EX2033 ¶¶133-36.

(b) *Hayhurst's Delivery Method Is Incompatible with Foster's System.*

The principal application for Foster's method is real-time cable television broadcasting to a set-top box.

As Dr. Rubin explains, Foster seeks to securely stream content, *e.g.*, live television, to a set-top box without the delay found in previous systems due to lack of synchronization between each packet and the key needed to decrypt it:

Foster's system serves as an intermediary between "source 428" and "recipient 430," where the "source" includes "a cable service provider" (EX1006, [0039], [0042]) and the "recipient" includes a "set-top box" (*id.*, [0040], [0041]. As Dr. Bhattacharjee agrees, Foster specifically seeks to improve upon the "Conditional Access System (CAS)," "such as a cable or satellite television system." *See id.*, [0052]; EX2034 41:10-15, 30:8-10. Consequently, Foster's principle of operation concerns delivering live cable television to a set-top box. EX2039 (CAS used for OTT digital video streaming service, "such as live sports"); EX2040 (CAS used for "content [transmitted] as a signal, which virtually anyone can pick up via satellite, terrestrial, or cable network."); *see* EX1006 [0056] (Foster seeks to avoid delays "when a channel is changed"); *see also* EX2034 37:11-39:9.

Foster's system is able to deliver live or real-time content as required for cable television because Foster's methods do not require a user to have an entire media file before it can view content. Rather, Foster's system allows viewers to receive and process packets in real-time as

they are generated and sent by the content provider. EX1006 [0065] (“the teachings of the present invention can be applied to the scenario where the content is received as content units”); EX2035, 220 (“In streaming, multimedia data is transferred in a stream of packets that are ***interpreted and rendered in real time*** by a software application, ***as the packets arrive in the user’s terminal.***” As a result, Foster avoids “delay[s]” “between when encrypted content is received and when it [is] accessed (e.g., between when a channel is changed and when an image is displayed).” *Id.*, [0056].

EX2033 ¶¶137-38.

Petitioner contends that “POSAs would have had numerous reasons” to store Foster’s encrypted content units on multiple storage devices (*e.g.*, consumer set-top boxes like Hayhurst’s subscriber units and Foster’s recipients 430) among the various subscribers in Hayhurst’s subscriber network. Pet., 62. But doing so would render the combination inoperable for viewing streamed content, Foster’s intended purpose, because Hayhurst requires that all segments be delivered to a requesting unit before the content can be reassembled and playback can begin. As Dr. Rubin explains:

Hayhurst is directed toward delivering video-on-demand and not live television. In particular, Hayhurst’s focus is upon delivering movies—*i.e.*, an already defined media file—in a fashion that avoids bandwidth limitations. EX1007 [0003]-[0004]. As such, Hayhurst can utilize a

decentralized delivery system in which segments of a movie are stored on set-top boxes throughout Hayhurst's system until one set-top box requests the entire movie. *Id.*, Abstract, [0006], [0028]. When a requesting set top box requests a movie, it cannot be played immediately. Rather, viewing can only begin after all segments are received, because "the segments are separate in the sense that they represent discontinuous or non-sequential portions of the movie and must be soiled and integrated with the remaining segments (distributed elsewhere in the network) to provide the complete movie."; EX2034 104:2-13. There is no indication in Hayhurst that the segments arrive in order to the requesting unit. Nor would it be feasible for Hayhurst's main server to facilitate such a thing, as there would be significant delays incurred as the main server would have to ensure successfully receipt of each segment before directing the next subscribing to send to following segment. Thus, only after all segments are received from the different members of the subscriber network can authorization to decode them be sought and obtained, and the segments are assembled and processed. *Id.*, [0028]-[0030].

EX2033 ¶140.

Because all segments must be received before the content can be reassembled and displayed, Foster/Hayhurst would not be able to broadcast live television. As Dr. Rubin explains:

In the Foster/Hayhurst combination, a set-top box requesting cable television content would have to wait to receive all of the packets sent

from the set-top boxes of a multitude of other subscribers before seeking and obtaining authorization and before reassembling and processing the entire content file. This wait-and-see approach would not work when trying to watch live television. EX1006 [0063].

EX2033 ¶141.

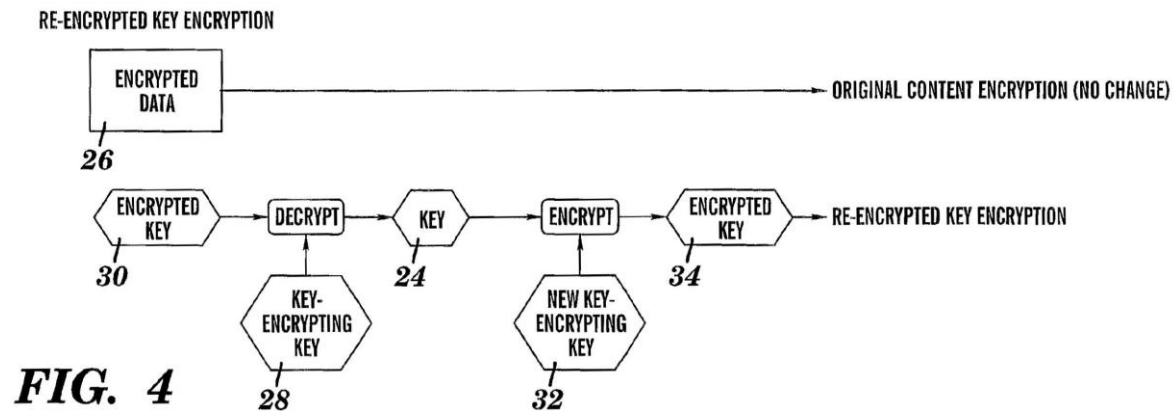
(c) *Hayhurst's Methods Make Foster's System Less Secure.*

Foster's content units are encrypted with title keys which are, in turn, encrypted with a key-encrypting-key ("KEK"). Pet., 65-66. In Petitioner's proposed Foster/Hayhurst combination, the encrypted content units would be, as in Hayhurst, distributed across thousands of subscribers. *Id.* A POSITA would not be motivated to do this because it would compromise the security of the system, as compared to Foster, by making Foster's KEKs more vulnerable while eliminating the ability (as disclosed in Foster) to change the KEK as necessary.

Because Foster teaches attaching the title key used to encrypt content to the content unit, the title key itself must also be encrypted with a KEK. See EX1006 [0053]. Critically, however, the KEK may be replaced if, *e.g.*, it is compromised.

As Dr. Rubin explains:

In Foster, should a key-encrypting-key be compromised or "protection on the content [need] to be varied," "an encrypted title key 30 can be re-encrypted with a different key encrypting key 32 without having to re-encrypt the encrypted content 26." EX1006 [0054].



Id., Fig. 4. Thus, Foster contemplates seamlessly switching the KEK for security purposes without re-encrypting the underlying content. Thus, if a key-encrypting-key is compromised, or a switch is otherwise desirable, a new KEK may be utilized going forward.

Moreover, Foster allows for a KEK to be unique to each recipient. Foster teaches that “key encrypting key 28 is generally determined based on a key management block (KMB), which is typically delivered to a recipient concurrently with or prior to the delivery of encrypted content 26.” *Id.*, [0054]. Because each recipient receives a KMB from which a KEK can be determined, that KEK can be unique to each recipient. This further increases the security of Foster’s content as the damage from any compromise of a recipient’s KEK can be limited to that recipient and further prevented by simply changing that recipient’s key-encrypting-key.

EX2033 ¶¶143-44.

Adding Hayhurst's method of storing and distributing content to Foster's system, however, both increases the likelihood that KEKs become compromised and interferes with Foster's ability to swap out a KEK as necessary. As Dr. Rubin explains:

Foster/Hayhurst uses Hayhurst's method of storing and distributing content. Consequently, any subscriber (of thousands) is able to request content that has been divided into segments across thousands of subscribers. Because any one of Hayhurst's subscribers can request the content, which has already been segmented and divided in advance, in any combination Foster's content units would all have to be secured using the same KEK(s), regardless of which subscriber will eventually request the content.

This, however, makes the combined system less secure for two reasons. *First*, it makes the KEKs more vulnerable. Because the KEK(s) is/are distributed amongst thousands of subscribers, there are thousands of potential points of failure. And, if one set-top-box (of thousands) with the KEK(s) gets compromised, all of the content is compromised because all of the content is encrypted using the same KEK(s) and title keys. *Second*, it would be more complicated to switch KEKs than in Foster alone as all of the content units are distributed across the subscribers instead of streamed in real time as in Foster. Thus, adding Hayhurst's methods to Foster's system would make Foster's system less secure in contravention of Foster's aims. EX1006 [0004] ("In

transmitting such content, however, the security thereof must be ensured.”).

EX2033 ¶¶145-46.

(d) *Petitioner Fails To Prove That The Alleged Benefits Outweigh The Drawbacks Of The Proposed Combination.*

As Dr. Rubin explains, the drawbacks to Petitioner’s proposed combination outweigh any alleged benefits:

Petitioner argues that a POSITA would be motivated to combine Foster and Hayhurst as proposed because Hayhurst’s methods would reduce bandwidth requirements, provide more security, and support redundancy. Pet., 62-63. Petitioner also argues that Hayhurst’s methods result in aggregate speed and efficiency/intelligence. *Id.*, 63.

Foster’s system, however, has no need for any of these alleged benefits. Foster’s system simply processes content and transmits streamed content to a particular recipient. EX1006 Fig. 16; [0078]. Because Foster’s system focuses upon streamed content (or content stored on a DVD), and provides a one-to-one transmission from Foster’s system to a particular recipient, there is no indication that Foster’s system suffers from the bandwidth constraints confronted by Hayhurst’s video-on-demand system. Foster’s system, moreover, has sufficient security at the source, security which would be undermined in the combination, as discussed previously. Further, Foster’s system has no need for redundancy as Foster’s system can simply resend dropped packets, nor

any need for efficiency/intelligence when sending on a one-to-one basis.

Moreover, any benefits are easily outweighed by the drawbacks. Again, Foster is directed towards reducing delays, particularly delays frustrating random access to content. The Foster/Hayhurst combination, however, would introduce enormous delays preventing random access to content and rendering Foster's system unsuitable for streaming live television. Further, the combination would also decrease Foster's security by exposing KEKs and hindering Foster's ability to replace a KEK when desirable.

EX2033 ¶147-49.

Petitioner, however, has failed to even consider much less weigh these manifold drawbacks against these purported benefits. For this additional reason, Petitioner fails to demonstrate that a POSITA would be motivated to combine Foster/Hayhurst as proposed.

C. Petitioner's Foster-Hayhurst Combination Fails Because Neither Foster Not Hayhurst Disclose "Data Chunks."

As explained earlier, Foster does not disclose generating the claimed "data chunks." *See supra* Section III.A.2.a.i. In the ID, the Board noted that the limitation was met due to "Hayhurst's disclosure of storage devices storing segments of one or more media files[.]" We respectfully disagree. Petitioner expressly relies on only Foster for the alleged generation of data shares and chunks and relies on Hayhurst

for storing and distributing Foster’s encrypted content units. Pet., 64; *see also* 62 (“POSAs would have been motivated to configure Foster’s content provider... as taught by Hayhurst”), 63 (combination involves “*Foster’s* encryption system to generate encrypted data segments, and *Hayhurst’s method for storing* encrypted data segments on multiple distributed storage devices ... to yield the predictable result of *Foster’s encrypted content units* being *stored ... as taught in Hayhurst.*”). To the extent, moreover, that Petitioner changes its combination to rely upon Hayhurst’s segments as the shares (and encrypted segments as the chunks), Hayhurst is of no help either. Hayhurst’s segments are also data packets. EX1007 [Hayhurst] [0020] (“*a segment is a digital packet* that includes data representing a small portion of the movie (video and audio)”). Thus, for the same reasons that Foster’s packet payloads are not shares and encrypted packet payloads are not chunks, Hayhurst’s segments are also not shares (or chunks when encrypted).

CONCLUSION

Petitioner fails to demonstrate by a preponderance of the evidence that any of the claims are invalid.

Date: September 12, 2024

Respectfully submitted,

/s/ Stephen J. Elliott

Stephen J. Elliott (Reg. No. 52,858)

Andrei Iancu (Reg. No. 41,862)

SULLIVAN & CROMWELL LLP

Kenneth J. Weatherwax (Reg. No. 54,528)

Nathan Lowenstein, *pro hac vice*

Colette Woo, *pro hac vice*

LOWENSTEIN & WEATHERWAX LLP

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Response (the “POR”) consists of 13,974 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The POR complies with the type-volume limitation of 14,000 words as mandated in 37 C.F.R. § 42.24. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Date: September 12, 2024

Respectfully submitted,

/s/ Stephen J. Elliott

Stephen J. Elliott (Reg. No. 52,858)

Andrei Iancu (Reg. No. 41,862)

SULLIVAN & CROMWELL LLP

Kenneth J. Weatherwax (Reg. No. 54,528)

Nathan Lowenstein, *pro hac vice*

Colette Woo, *pro hac vice*

LOWENSTEIN & WEATHERWAX LLP

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served by electronic service, by agreement between the parties, on the date below:

PATENT OWNER RESPONSE

EXHIBITS 2033-2041

The names and addresses of the parties being served are as follows:

Elisabeth H. Hunt	EHunt-PTAB@wolfgreenfield.com
Richard F. Giunta	RGiunta-PTAB@wolfgreenfield.com
Marc S. Johannes	MJohannes-PTAB@wolfgreenfield.com

Date: September 12, 2024

Respectfully submitted,

/s/ Stephen J. Elliott

Stephen J. Elliott (Reg. No. 52,858)

Andrei Iancu (Reg. No. 41,862)

SULLIVAN & CROMWELL LLP

Kenneth J. Weatherwax (Reg. No. 54,528)

Nathan Lowenstein, *pro hac vice*

Colette Woo, *pro hac vice*

LOWENSTEIN & WEATHERWAX LLP