

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case IPR2024-00212
Patent 11,178,116

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. OVERVIEW OF THE '116 PATENT AND THE CHALLENGED CLAIMS.	2
III. THE TAJIMA GROUNDS FAIL (ALL CLAIMS, GROUND 1-4).....	3
A. Petitioner Fails To Show That Tajima Discloses Or Renders Obvious “Separately Storing Each Data Chunk ... On A Plurality Of Different Storage Devices” (All Claims, Grounds 1-4).....	3
B. Petitioner Fails To Show That Tajima Discloses Or Renders Obvious “Separately Storing Each Data Chunk ... Together With One Of The Plurality Of [Obfuscated/Transformed] Different Encryption Keys” (All Claims, Grounds 1-4).....	12
IV. THE FOSTER-HAYHURST GROUND FAILS (ALL CLAIMS, GROUND 5).	24
A. The '116 And Foster Fundamentally Differ.....	25
B. Petitioner’s Proposed Foster-Hayhurst Combination Does Not Disclose The Limitations Of The Independent Claims (All Claims).	27
1. Foster-Hayhurst Does Not Disclose Or Render Obvious The Preamble Limitation Of The Independent Claims, Under The Parties’ Agreed Construction (All Claims).	27
2. Petitioner Fails To Show Foster Discloses “Distributing The Data Set Into A Plurality Of Data Chunks” (All Claims).	28
3. Foster Does Not Disclose Or Render Obvious “Separately Storing Each Data Chunk Of The Plurality Of Data	

Chunks . . . On A Plurality Of Different Storage Devices”
(All Claims).....34

V. CONCLUSION 38

TABLE OF AUTHORITIES

Page(s)

COURT DECISIONS

<i>Allergan, Inc. v. Apotex Inc.</i> , 754 F.3d 952 (Fed. Cir. 2014)	11
<i>Archer Daniels Midland Co. v. United States</i> , 561 F.3d 1308 (Fed. Cir. 2009)	37
<i>Arctic Cat Inc. v. Polaris Indus.</i> , 795 F. App'x. 827 (Fed. Cir. 2019)	22
<i>Arendi S.A.R.L. v. Apple, Inc.</i> , 832 F.3d 1355 (Fed. Cir. 2016)	19
<i>BlephEx, LLC v. Myco Indus.</i> , 24 F.4th 1391 (Fed. Cir. 2022)	18
<i>DSS Tech. Mgm't v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	19
<i>Finisar Corp. v. DirecTV Group, Inc.</i> , 523 F.3d 1323 (Fed. Cir. 2008)	18
<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016)	16
<i>Henny Penny Corp. v. Frymaster LLC</i> , 938 F.3d 1324 (Fed. Cir. 2019)	22
<i>HTC Corp. v. Cellular Commns. Equip., LLC</i> , 877 F.3d 1361 (Fed. Cir. 2017)	5, 14
<i>IBM v. Iancu</i> , 759 Fed. App'x. 1002 (Fed. Cir. 2019)	37

<i>In re Conrad</i> , 759 Fed. App'x. 982 (Fed. Cir. 2019)	24
<i>In re Hughes</i> , 345 F.2d 184 (CCPA 1965)	11
<i>In re Kahn</i> , 441 F.3d 977 (Fed. Cir. 2006)	7
<i>In re Magnum Oil Tools Int'l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	7
<i>In re Oelrich</i> , 666 F.2d 578 (CCPA 1981)	8
<i>In re Ratti</i> , 270 F.2d 810 (CCPA 1959)	22
<i>In re Robertson</i> , 169 F.3d 743 (Fed. Cir. 1999)	8
<i>In re Turlay</i> , 304 F.2d 893 (CCPA 1962)	11
<i>InTouch Techs., Inc. v. VGo Commc'ns., Inc.</i> , 751 F.3d 1327 (Fed. Cir. 2014)	24
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	7
<i>LBT IP I LLC v. Apple Inc.</i> , 2023 U.S. App. LEXIS 14376 (Fed. Cir. 2023)	5, 14
<i>Microsoft Corp. v. Biscotti, Inc.</i> , 878 F.3d 1052 (Fed. Cir. 2017)	5, 14
<i>Net MoneyIN, Inc. v. VeriSign, Inc.</i> , 545 F.3d 1359 (Fed. Cir. 2008)	11, 18
<i>Otsuka Pharm. Co., v. Sandoz, Inc.</i> , 678 F.3d 1280 (Fed. Cir. 2012)	23

<i>Par Pharm., Inc. v. TWi Pharms., Inc.</i> , 773 F.3d 1186 (Fed. Cir. 2014)	8
<i>Plas-Pak Indus., Inc. v. Sulzer Mixpac AG</i> , 600 F. App'x. 755 (Fed. Cir. 2015)	22
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	22
<i>Ruiz v. A.B. Chance Co.</i> , 357 F.3d 1270 (Fed. Cir. 2004)	23
<i>Schumer v. Lab. Computer Sys., Inc.</i> , 308 F.3d 1304 (Fed. Cir. 2002)	6, 7
<i>Shoes by Firebug LLC v. Stride Rite Children's Grp., LLC</i> , 962 F.3d 1362 (Fed. Cir. 2020)	27
<i>Unigene Labs., Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	11
<i>Univ. of Strathclyde v. Clear-Vu Lighting LLC</i> , 17 F.4th 155 (Fed. Cir. 2021)	23
<i>Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.</i> , ___ F.4th ___, Case No. 2022-1998 (Fed. Cir. Mar. 27, 2024)	7, 30
<i>W.L. Gore & Assocs., Inc. v. Garlock, Inc.</i> , 721 F.2d 1540 (Fed. Cir. 1983)	11
<i>Wasica Fin. GmbH v. Cont'l Auto. Sys.</i> , 853 F.3d 1272 (Fed. Cir. 2017)	11

AGENCY DECISIONS

<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (Aug. 24, 2022) (precedential)	7, 8, 30
--	----------

REGULATIONS

37 C.F.R. § 42.6(a)(3) 7

EXHIBIT LIST	
2001-2002	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]
2012-2013	Reserved
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]
2017-2018	Reserved
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 (Non-Confidential Redacted Version) (Jan. 8, 2024) [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) [Cambridge-Dictionary]
2022	Reserved
2023	Excerpts from Oxford University Press, <i>Oxford English Dictionary</i> (12th ed. 2012) [Oxford-English-Dictionary]
2024	Excerpts from HarperCollins Publishers, <i>English Dictionary for Advanced Learners</i> (3d ed. 2001) [Collins-Dictionary]
2025	Japanese Patent Application Publication No. JP2003046500A to Tajima <i>et al.</i> [Tajima-Japan-Application]
2026	Cambridge Dictionary, 登録, https://dictionary.cambridge.org/us/dictionary/japanese-english/%E7%99%BB%E9%8C%B2 (last visited Mar. 22, 2024) [Cambridge-Japanese-English-Dictionary]

2027	TechTarget, <i>Certificate Authority</i> , https://www.techtarget.com/searchsecurity/definition/certificate- authority (last updated Sept. 2021) [TechTarget]
------	---

I. INTRODUCTION

The Petition should be denied as it fails to demonstrate a reasonable likelihood of prevailing as to at least one of the challenged claims under either of the grounds on which Petitioner relies. *See* Sections III-IV.

Four out of Petitioner's five grounds rely upon the Tajima reference as allegedly teaching most, if not all, of the recited limitations. Petitioner, however, fails to demonstrate that Tajima discloses and/or renders obvious multiple limitations. Rather, Petitioner relies upon disclosures in Tajima that at best are ambiguous and in fact disclose the opposite of what the claims require. *See* Section III.

Petitioner's remaining ground relies upon the Foster reference as the primary reference. Foster, however, is a fundamentally different invention than the '116's claimed inventions. Foster concerns streaming content between content owners, such as a movie studio, and consumer receivers, such as a set-top box. The '116, by contrast, concerns long-term, secure storage of data. This fundamental difference between Foster and the '116 pervades Petitioner's arguments and consequently, Petitioner fails to demonstrate that its Foster-Hayhurst combination teaches multiple limitations. *See* Section IV.

II. OVERVIEW OF THE '116 PATENT AND THE CHALLENGED CLAIMS.

The '116 relates to, *inter alia*, securing data within a system for long-term storage. As Dr. Rubin explains:

The '116's claimed inventions, and related disclosure, concern securing data within a system. Ex. 1001 ['116] 1:28-33 (“computer systems . . . are often storing, archiving, and transmitting all types of sensitive information. Thus, an ever-increasing need exists for ensuring data stored and transmitted over these systems cannot be read or otherwise compromised.”). The '116 further teaches that it is undesirable for stored data to “remain[] whole and intact and subject to attack.” *Id.*, 57:12-13. To address this need, the '116 teaches methods in which a dataset is processed with a “cryptographic parsing and splitting . . . into two or more portions or shares,” secured with “another layer of encryption to each share of the data,” and then stored such that shares are in “different physical and/or logical locations.” *Id.*, 57:14-24.

In accord, the claims require parsing the dataset into chunks, encrypting those chunks with distinct encryption keys, obfuscating or transforming those encryption keys, and then storing the data chunks on a plurality of different storage devices. *Id.*, cls. 1, 9. Each of these steps is intended to secure the dataset. “[C]ryptographic parsing and splitting” of the dataset into chunks and “physical[] remov[al]” the encrypted and “further secure[d]” chunks from the system onto a

plurality of different storage devices removes the possibility of “attack” or “compromise” of the whole dataset. *Id.*, 57:13-24.

Ex. 2003 [Rubin-Decl.] ¶¶ 33-34. For the reasons explained below, Petitioner fails to demonstrate that its Tajima or Foster-based grounds teach multiple limitations.

III. THE TAJIMA GROUNDS FAIL (ALL CLAIMS, GROUND 1-4).

Petitioner contends that Tajima anticipates and/or renders obvious each of the claims (Ground 1). Petitioner, however, fails to demonstrate that Tajima satisfies multiple claim limitations. *See* Section III.A-B.

A. Petitioner Fails To Show That Tajima Discloses Or Renders Obvious “Separately Storing Each Data Chunk ... On A Plurality Of Different Storage Devices” (All Claims, Grounds 1-4).

Both of the independent claims require “separately storing each data chunk of the plurality of data chunks together with one of the plurality of [obfuscated/transformed] different encryption keys on a plurality of different storage devices.” Ex. 1001 [’116] cls. 1, 9. Notably, in prosecution, the claims were allowed after this limitation was amended to require “separately storing each data chunk of the plurality of data chunks together with one of the plurality of [obfuscated/transformed] different encryption keys on a plurality of different storage devices.” *See* Ex. 1002 [Pros. Hist.] 118-122 (amended claims) (underlining in original), 93-98 (notice of allowance).

For each of Grounds 1-4, Petitioner relies upon Tajima as disclosing “separately storing each data chunk ... on a plurality of different storage devices.” Pet., 11-12, 23-24; *see also id.*, 40-41, 44, 47, 49. Petitioner identifies Tajima’s “encrypted data fragments X and Y” as the data chunks. *Id.*, 11-12. Petitioner further relies upon Tajima’s teaching that these fragments are “separately **‘registered’**” in databases 41a and 41b as satisfying the requirement that each data chunk is stored on a “plurality of different storage devices.”¹ *Id.*

Notably, however, Tajima never says that its data fragments are “**stored**” in databases 41a and 41b. Rather, Tajima indisputably, consistently, and repeatedly tells us the data fragments are “**registered.**” Pet., 23 (“Tajima’s ... **registering** the resulting data fragments on respective different databases meets [1D]”); *see, e.g.*, Ex. 1005 [Tajima] Fig. 6 (S6: “**register** data fragment X”), [0101] (“Data fragment X is then **registered** with database 41a of certificate authority 40a”); [103] (same); [106] (similar); [0111] (“encrypted data fragment X is then **registered** with database 41a of certificate authority 40a”), [0113] (similar), [0115] (“data fragment X in which personal information has been divided is **registered** with certificate authority 40a”).

¹ All emphasis added unless otherwise stated.

Petitioner, nonetheless, contends that “registering” necessarily entails “storing.” Pet., 23 (“*POSAs understood* that ... *registering a data fragment with a data base includes storing it...*”). Similarly, Petitioner’s expert, Dr. Bhattacharjee, contends that “[a] *POSA understood that when a data fragment is ‘registered’ with a data base the data fragment is stored* on the corresponding storage media,” and that while “[r]egistering may also include additional processes that databases conventionally use to record information ... the principal act of registering data with a database is storing the data so that it can be accessed as authorized.” Ex. 1003 [Bhattacharjee-Decl.] ¶ 71.

Petitioner’s argument, thus, is that when Tajima says it “registers” a data fragment, a POSITA would have “understood” that this includes storing the fragment. Petitioner and its expert provide no basis for this conclusory opinion. The argument concerning what a POSITA would have “understood” lies in inherency. *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] ...”); *LBT IP I LLC v. Apple Inc.*, 2023 U.S. App. LEXIS 14376, *8 (Fed. Cir. 2023) (similar). This requires a showing that the limitation is “*necessarily* present” in the allegedly invalidating reference. *HTC Corp. v. Cellular Commns. Equip., LLC*, 877 F.3d 1361, 1368-69 (Fed. Cir. 2017).

Thus, Petitioner must prove that when Tajima “registers” a data fragment, it **necessarily** stores the fragment in or “on” the database. Neither Petitioner nor its expert, however, cite anything in Tajima to prove that Tajima’s registration of data fragments in different databases necessarily entails storing the data fragments in those databases. Dr. Bhattacharjee’s statement that “[a] POSA understood that when a data fragment is ‘registered’ with a data base the data fragment is stored on the corresponding storage media,” is unsupported *ipse dixit*. Not only does he not point to any evidence in Tajima supporting his view, but he also does not point to any other evidence proving that Tajima’s registering **necessarily** entails storing.

In fact, Petitioner’s expert does not even state that the data fragments are stored **on** databases 41a and 41b. He only posits that “[a] POSA understood that when a data fragment is ‘registered’ with a data base **the data fragment is stored on the corresponding storage media.**” Ex. 1003 [Bhattacharjee-Decl.] ¶ 71.

Importantly, however, Petitioner’s expert does not say what the “corresponding storage media” is or provide any indication that this corresponding storage media is, necessarily, databases 41a and 41b or any other “plurality of different storage devices.” The expert’s conclusory testimony is insufficient to show disclosure. *Schumer v. Lab. Computer Sys., Inc.*, 308 F.3d 1304, 1315-16 (Fed. Cir. 2002) (“testimony [concerning anticipation] is insufficient if it is merely conclusory.”);

Xerox Corp. v. Bytemark, Inc., IPR2022-00624, Paper 9, 15-16 (Aug. 24, 2022) (precedential).

It is well-settled that anticipation/obviousness may not be shown through conclusory statements. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)) (“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.”); *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.”).

Moreover, it is equally well-settled that an expert’s conclusory statements are insufficient to establish invalidity. See 37 C.F.R. § 42.6(a)(3) (unsupported expert testimony entitled to “little or no weight”); *Schumer*, 308 F.3d at 1315-16 (“testimony [concerning anticipation] is insufficient if it is merely conclusory.”); *Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.*, __ F.4th __, Case No. 2022-1998, slip op. at *7 n.2 (Fed. Cir. Mar. 27, 2024) (“the conclusory assertions in Dr. Mohazzab’s declaration do not provide substantial evidence for finding a motivation to combine.”). Indeed, Dr. Bhattacharjee’s argument that registering

necessarily includes storing is precisely the sort of conclusory testimony rejected in *Xerox*:

Petitioner’s only evidence in support of its assertion that blocking the purchaser would require recording the blocking in a record in the user’s account is the opinion of its Declarant, Dr. Jones. ... Dr. Jones does not cite to any additional supporting evidence or provide any technical reasoning to support his statement. Thus, the cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight.

Xerox Corp. v. Bytemark, Inc., IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential) (emphasis in original, citations omitted).

Petitioner’s and its expert’s conclusory statements are particularly insufficient to demonstrate that a limitation is inherently met. Inherency, again, is a demanding standard that “may not be established by probabilities or possibilities.” *Par Pharm., Inc. v. TWi Pharms., Inc.*, 773 F.3d 1186, 1195 (Fed. Cir. 2014) (“Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.”) (cleaned up) (quoting *In re Oelrich*, 666 F.2d 578, 581 (CCPA 1981)); *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (same).

This is sufficient to reject Petitioner’s claim that Tajima discloses “separately storing each data chunk ... on a plurality of different storage devices.” But in addition to being unsupported by evidence, Petitioner’s argument also fails on the merits because a POSITA would not understand that “registering” a data fragment in a database necessarily entails “storing” the fragment itself in or on the database or on a “corresponding” storage device. As Dr. Aviel Rubin explains:

Tajima’s use of the term “register” does not necessarily indicate storing the data itself. In multiple places, Tajima describes “registering *the user* of user terminal 510 with certificate authority 540.” Ex. 1005 [Tajima] [0030]; *e.g., id.*, [0038] (“when a user [] *has registered with certificate authority 540*”), [0053] (“FIG. 4 is a flow chart, for explaining the process of *registering the user* of a user terminal to a certificate authority with the information processing system shown in FIG. 3”). It is hardly possible, let alone necessarily true, that a user can be “stor[ed]” “on” the certificate authority’s database as the claims require.

In this regard, Tajima appears to use the verb “register” in accord with customary usage wherein a record corresponding to or pointing to a thing, rather than the thing itself, is stored. *See, e.g.,* Ex. 2023 [Oxford-English-Dictionary] 608 (register (verb): “1 enter someone or something in an official list or record. 2 put your name on an official list or record”); Ex. 2024 [Collins-Dictionary] 1297 (“If you **register** something, such as the name of a person who has just died or information about something you own, you have these facts recorded

in an official list.”). I have been informed that a dictionary definition for the Japanese characters used in the original Japanese application (*E.g.*, Ex. 2025 [Tajima-Japan-Application] 1:3 (using “登録”)) accords with these definitions. *E.g.*, Ex. 2026 [Cambridge-Japanese-English-Dictionary] (defining 登録 as “registration”: “the act of recording names or information on an official list”). Thus, given the customary meaning of the term “register,” along with the way the term is used in Tajima itself, a POSITA would understand that “registering” a data fragment in databases 41a and 41b simply means storing a record or pointer corresponding to the data fragment in the database, rather than the data fragment itself.

Consequently, a POSITA reading Tajima would not understand it to teach “storing” a data fragment when it uses the term “registering.”

Ex. 2003 [Rubin-Decl.] ¶¶ 45-47.

Thus, Tajima does not disclose “storing” the data fragments on the plurality of different storage devices; it merely discloses “registering” the data fragments. This is important—the whole point of the ’116 patent is to secure chunks of a data set that are stored on storage devices. *See* Section II. The claims-at-issue are not about registering data fragments or even securing such registers in the abstract.²

² Tajima certainly does not indicate that the data itself is stored securely or that the security protocol is performed on the data set. At best, Tajima’s disclosure

In sum, Tajima discloses “registering,” not “storing.” Petitioner asserts, but does not prove, that “registering” entails “storing” much less that this is necessarily so. To the contrary, Tajima does not seem to use “registering” in this fashion but rather in accord with the common usage of to “register” wherein some information corresponding to a thing rather than the thing itself is recorded. Petitioner’s

is arguably ambiguous in this regard. But the Federal Circuit has consistently held that “ambiguous references do not, as a matter of law, anticipate a claim.” *Wasica Fin. GmbH v. Cont’l Auto. Sys.*, 853 F.3d 1272, 1284 (Fed. Cir. 2017) (citing *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554 (Fed. Cir. 1983) (refusing to find claims anticipated when the prior art references were “unacceptably vague”)); *Allergan, Inc. v. Apotex Inc.*, 754 F.3d 952, 959-60 (Fed. Cir. 2014) (affirming finding that “disclosure was too sparse and ambiguous for a person of ordinary skill to comprehend Johnstone’s disclosure as anticipating the ’029 patent.”) (citing *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008)); *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1361 (Fed. Cir. 2011) (similar); see also *In re Hughes*, 345 F.2d 184, 188 (CCPA 1965); *In re Turlay*, 304 F.2d 893, 899 (CCPA 1962) (“It is well established that an anticipation rejection cannot be predicated on an ambiguous reference.”).

conclusory and ambiguous arguments to the contrary cannot demonstrate anticipation or obviousness, particularly when based on inherency. This alone is sufficient reason to reject Petitioner's Tajima grounds.

B. Petitioner Fails To Show That Tajima Discloses Or Renders Obvious “Separately Storing Each Data Chunk ... Together With One Of The Plurality Of [Obfuscated/Transformed] Different Encryption Keys” (All Claims, Grounds 1-4).

The independent claims both require “storing each data chunk ... together with one of the plurality of [obfuscated/transformed] different keys.” Ex. 1001 [’116] cls. 1, 9. In each of its Tajima-based grounds, Petitioner argues that Tajima discloses and/or renders obvious this limitation by teaching attaching “key information” or “information regarding the key” 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 ...”); *see also* 40-41, 44, 47, 49. As used in Tajima, however, “key information” or “information regarding the key” is distinct from the key itself, and thus, Tajima does not teach “storing each data chunk ... together with one of the plurality of [obfuscated/transformed] different keys.”

Petitioner relies entirely upon Tajima's teachings regarding the embodiments disclosed in Figures 12 and 13 of the reference, wherein

“[i]nformation regarding the key that was used for the encryption” is attached to a data fragment:

Fig. 12

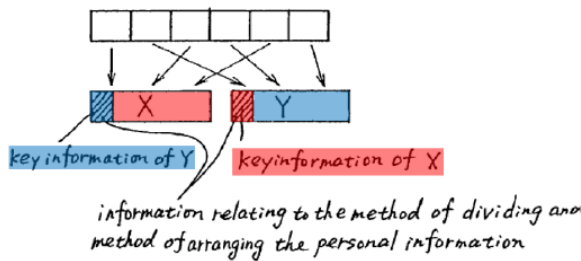
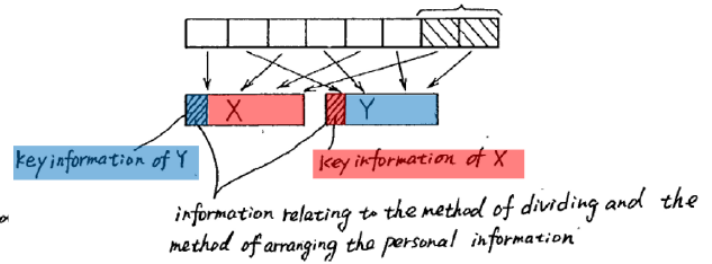


Fig. 13



Pet., 19-20 (citing Ex. 1005 [Tajima] Figs. 12, 13); Ex. 1005 [Tajima] [0111]

(“**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.”), [0113] (similar), [0112] (“**key information** that has been attached to the encrypted data fragment X”), [0114] (similar).

Recognizing that Tajima does not expressly disclose the limitation, 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 for several reasons.” Pet., 20 (citing only Ex. 1003 [Bhattacharjee-Decl.] ¶ 96) (emphasis in original). Thus, Petitioner does not contend that Tajima expressly discloses storing a key with the data fragments, but rather contends that Tajima

discloses attaching “information regarding the key” to the data fragments and that a POSITA “understood” this means the key is stored with the data fragments. But this is not what a POSITA would understand from Tajima’s disclosure.

First, as discussed above, an argument about what a POSITA “understood” from a disclosure lies in inherency. *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] ...”); *LBT IP I LLC v. Apple Inc.*, 2023 U.S. App. LEXIS 14376, *8 (Fed. Cir. 2023) (similar). This, again, requires a showing that the limitation is “**necessarily** present” in the allegedly anticipating reference. *HTC Corp. v. Cellular Commns. Equip., LLC*, 877 F.3d 1361, 1368-69 (Fed. Cir. 2017).

Petitioner again fails to surmount this high bar based on Tajima’s disclosure. As Dr. Rubin explains:

Petitioner relies on Tajima’s teachings that “information regarding the key” is stored with the data fragments. I do not believe that, based on Tajima’s disclosure, a POSITA would understand this disclosure to necessarily refer to the key.

Indeed, when Tajima wishes to refer to a “key,” it does so. *E.g.*, Ex. 1005 [Tajima] [0070] (“In Step S1, the user of user terminal 10 first uses user terminal 10 to **create a public key and secret key** ..., and

further, submits **this public key** and personal information ... to certificate authority 40a in Step S2.”), [0071] (“Upon receiving **the public key** and personal information in Step S3”); [0075], [0077], [0086] (“the user ... uses **the secret key** that was created in Step S1 (see FIG. 6) to encrypt the compressed permit”), [0088] (“Store 20 then uses **the acquired public key** to check whether the received permit was created by the user”), [0089] (“store 20 first uses **the public key** that was acquired in Step S28 to decrypt the encrypted permit”).

Instead, Tajima’s disclosure of “key information” or “information **regarding** the key” appears to refer to information about the key, not the key itself. At best, Tajima’s use of “key information” or “information regarding the key” is somewhat ambiguous. What is clear, however, is that when Tajima wishes to refer to a “key” it does so, and I do not believe a POSITA would conclude that Tajima **necessarily** sends the key when it sends “information regarding the key.”

Ex. 2003 [Rubin-Decl.] ¶¶ 54-56.

Petitioner also argues that because “Tajima never says that anything else beyond the key information is needed for decrypting the corresponding data fragment and does not disclose any additional steps nor any separate key management infrastructure,” then “the key information includes the key.” Pet., 20-21. But Tajima’s lack of disclosure is at best ambiguous and does not say anything about where the key is stored, and it certainly does not establish that the key is

necessarily included with the key information. *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”). And, as Dr. Rubin explains:

Petitioner and Dr. Bhattacharjee seem to be relying upon Tajima’s silence regarding key management. They note that Tajima “does not disclose any additional steps nor any separate key management infrastructure” and conclude from this silence that “information regarding the key” must include the key itself. Pet., 20-21. This does not logically follow. All Tajima is telling us is that, arguably, “information regarding the key” may be stored with the data fragment. It is silent concerning where the key is stored. Nothing in that silence indicates that the key is stored with the data fragments, much less that this is necessarily so. And that Tajima does not set forth its key management infrastructure only goes to show that Tajima does not specify where the keys are stored.

Moreover, Petitioner’s argument seems based upon the assumption that storing Tajima’s encryption keys apart from the encrypted data fragments would require a “*separate*” key management infrastructure that would be set forth in Tajima itself. Pet., 20-21. But Tajima is based in and improves upon a prior art certificate authority system (see Ex. 1005 [Tajima] Fig. 3) which already includes key management for both public keys and private (“secret”) keys. Ex. 2027 [TechTarget]. Thus, Tajima’s encryption keys could be readily stored

in a preexisting key management infrastructure Tajima alludes to in the prior art.

Petitioner also relies on Tajima's statements that "information regarding the key" "is used to decrypt" a data fragment. Ex. 1005 [Tajima] [0112], [0114]. But that does not establish whether the "information regarding the key" as disclosed in the Tajima reference necessarily includes the key itself. To the extent Tajima's "information regarding the key" includes information that can be used to fetch or derive the key (*e.g.*, information about where the key is stored, the type of key that is used, or other information that can be used to obtain the key) such information could readily be "used to decrypt" a data fragment without storing the key itself with the data fragment.

Ex. 2003 [Rubin-Decl.] ¶¶ 58-60.

Petitioner also argues that a claim of Tajima that Petitioner contends corresponds to Tajima's Figure 11 embodiment recites an "encryption key" where the disclosure regarding the Figure 11 embodiment recites "information regarding the key." Pet., 21. But the discussion of the Figure 11 embodiment does not shed light on what Tajima means by "information regarding the key" in the Figures 12 and 13 embodiments on which Petitioner relies. Nor does the Figure 11 embodiment appear itself to disclose the limitation-at-issue: in the Figure 11 embodiment, both the data and encryption key are split into fragments, and at best only a piece of the key is stored with a data fragment. Ex. 1005 [Tajima] [0109].

In any event, Petitioner does not rely on Figure 11, and Petitioner may not “mix and match” features from different embodiments of Tajima to argue that the claims are anticipated. “‘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.*, 24 F.4th 1391, 1400 (Fed. Cir. 2022); *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (anticipation requires “the limitations [be] arranged or combined in the same way as recited in the claim”); *Finisar Corp. v. DirecTV Group, Inc.*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) (similar).

Alternatively, Petitioner argues that “[e]ven if Tajima had not disclosed that its key information includes the corresponding key, that would have been an obvious and conventional way to implement what Tajima discloses—i.e., a system that needs only the key information to decrypt data fragments and not additional key management infrastructure.” Pet., 22 (citing Ex. 1003 [Bhattacharjee-Decl.] ¶ 104). But beyond its expert’s equally conclusory testimony, Petitioner offers no evidence or explanation of why attaching an encryption key itself to a data fragment “would have been an obvious and conventional way” to modify Tajima.

When a limitation is missing in the prior art, a court’s review of any purported “reasoned basis for resort to common sense” as the motivation for a modification of the reference must be “searching” *Arendi S.A.R.L. v. Apple Inc.*,

832 F.3d 1355, 1362-63 (Fed. Cir. 2016). What is more, “common sense” can 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, 1374-75 (Fed. Cir. 2018) (citations omitted). Here, “[t]he inventions-at-issue concern cryptography, which is a technologically-involved and complex field involving incredibly high stakes and safeguarding against a wide variety of highly sophisticated and ever-evolving cybersecurity attacks,” (Ex. 2003 [Rubin-Decl.] ¶ 65) and, thus, cannot be satisfied by purported common sense.

Nor is Petitioner’s proposed modification of Tajima simply the application of a “conventional” method. As Dr. Rubin explains:

The limitations-at-issue (and 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 Ex. 2010 [Schneier-Applied-Cryptography] 169 (“In the real world, key management is the hardest part of cryptography. Designing secure cryptographic algorithms and protocols isn’t easy, but you can rely on a large body of academic research. Keeping the keys secret is much harder.”); see also Ex. 2007 [Katz] 22 (“As an example, an encryption scheme that has been proven secure ... might be

implemented on a smart-card. It may then be possible for an adversary to monitor the power usage of the smartcard (e.g. how this power usage fluctuates over time) and use this information to determine the key.”); Ex. 2008 [Schneier-Security-Pitfalls-in-Cryptography] (“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.”); Ex. 2009 [Anderson] (new computer “security systems have a nasty habit of backfiring”).

Ex. 2003 [Rubin-Decl.] ¶ 66. Consequently, Petitioner’s attempt to rely solely on the common sense of a POSITA to modify Tajima should be rejected here because it cannot withstand the “searching” inquiry required to satisfy a missing limitation, particularly one that arises in a technically complex field.

Nor does Petitioner demonstrate that a POSITA would be motivated to make its alteration. To the contrary, as Petitioner itself later acknowledges, there are significant security drawbacks to modify Tajima to include the encryption key itself in the “information regarding the key” attached to the encrypted data fragment—encryption performed with one of the encryption keys. It is indeed counterintuitive to store encryption keys together with the encrypted data (it would make the system *less* secure, absent careful management as disclosed by the ’116 patent), and Petitioner and its expert do not in any way articulate why or how a POSITA would do that absent the inventions disclosed in the ’116 patent.

In addition, Tajima does not teach encrypting the encryption keys, and the Petition states that:

It was known that storing plaintext (i.e., unencrypted) keys with encrypted data results in a vulnerability. Bhattacharjee, ¶140, citing EX1021, 1:45-65 (explaining that simple-to-use methods “where the data encryption keys are stored or transmitted together with the encrypted data” are likewise potentially simple to defeat), EX1023, 17:44-18:8 (storing plaintext keys with the information that they protect “is somewhat akin to locking a house and then putting the keys under the doormat”); EX1022, 10:42-48 (“cryptographic keys should never occur in clear form outside the cryptographic device”).

... POSAs understood that by storing the key in plaintext, Tajima’s approach subjects the data fragments to risk because if an attacker is able to recover all of Tajima’s data fragments (e.g., both data fragments X and Y), the attacker will possess all the plaintext keys used to encrypt the entire data set. Bhattacharjee, ¶141. Decrypting the individual data fragments would become merely a matter of trying different key/data-fragment combinations, which was within the capabilities of hackers in the relevant timeframe. Bhattacharjee, ¶¶141-43 (describing known techniques to address the vulnerability of plaintext keys).

Pet., 33-34. Thus, contrary to Petitioner’s unsupported claim that it would be obvious to store the key with the data fragment, Petitioner itself shows that modifying Tajima to include an unencrypted key in the key information stored

with the data fragments would make Tajima's system less secure.

A POSITA would understand that Tajima did not mean to include the key itself in "information regarding the key" because attaching such information (and not key itself) to a data fragment has the security benefit that an attacker who obtains all of the data fragments still would not possess all of the keys necessary to decrypt those fragments. A POSITA would not be motivated to modify Tajima's system as Petitioner suggests because it would make the system less secure.

Polaris Indus., Inc. v. Arctic Cat, Inc., 882 F.3d 1056, 1069-70 (Fed. Cir. 2018) (reversible error to find motivation to combine where resulting combination "would run contrary to [the primary 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."); *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959) (no motivation to combine where "suggested combination of references would require . . . a change in the basic principles under which the [reference] was designed to operate."); *Arctic Cat Inc. v. Polaris Indus.*, 795 F. App'x. 827, 833 (Fed. Cir. 2019) ("The Board must weigh the benefits and drawbacks of the modification against each other, to determine whether there would be a motivation to combine."); *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1331-32 (Fed. Cir. 2019) (rejecting argument that "Board placed undue

weight on the disadvantages of introducing Iwaguchi's TPM sensor into Kauffman's system" where tradeoffs of combination may "yield an unappetizing combination").

Finally, Petitioner's proffered modification should be rejected because it appears to derive entirely from the '116's inventive concept of storing each data chunk with an obfuscated or transformed encryption key. *See, e.g.*, Ex. 1001 ['116] Fig. 21, 57:59-62 (teaching "stor[ing] the encryption keys in different locations from the encrypted data portions or shares"). Petitioner found a reference (Tajima) that it believes includes some of the elements of claim 1 of the '116 and proposes to modify that reference to include the other limitations, without offering a legitimate reason or motivation, and in direct contravention of the reference's disclosure. This is precisely the sort of hindsight-driven analysis, using the claims-at-issue as a roadmap, the Federal Circuit has rejected. *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."); *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 165 (Fed. Cir. 2021) ("[t]he inventor's own path itself never leads to a conclusion of obviousness; that is hindsight.") (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).

In sum, Petitioner fails to demonstrate that Tajima discloses or renders obvious "storing each data chunk ... together with one of the plurality of [obfuscated/transformed] different keys."

IV. THE FOSTER-HAYHURST GROUND FAILS (ALL CLAIMS, GROUND 5).

Petitioner's last ground argues the claims are anticipated and/or rendered obvious by Foster and Hayhurst. Pet., 1. Petitioner's primary reference, Foster, however, is a fundamentally different invention from the '116 and concerns protecting content streamed or transmitted from a content owner to a consumer rather than securing stored data as the '116 does. See Section IV.A. Not surprisingly, Petitioner's last ground also fails and for multiple reasons. See Section IV.B.

A. The '116 And Foster Fundamentally Differ.

The '116 and Foster arise in entirely different contexts, are directed towards addressing fundamentally different problems, and result in very different inventions. As Dr. Rubin explains:

The '116's claimed inventions, and related disclosure, concern securing data within a system. Ex. 1001 ['116] 1:28-33 (“computer systems . . . are often storing, archiving, and transmitting all types of sensitive information. Thus, an ever-increasing need exists for ensuring data stored and transmitted over these systems cannot be read or otherwise compromised.”). This is accomplished by the claimed method of parsing the dataset into chunks, encrypting those chunks with distinct encryption keys, obfuscating or transforming those encryption keys, and then storing the data chunks on a plurality of different storage devices. *Id.*, cls. 1, 9. Each of these steps is intended to secure the dataset. “[C]ryptographic parsing and splitting” of the dataset into chunks and “physical[] remov[al]” of at least one of the encrypted and “further secure[d]” chunks from the system onto storage devices removes the possibility of “attack” or “compromise” of the whole dataset. *Id.*, 57:13-24.

Foster, by contrast, is directed towards a system wherein a content owner (*e.g.*, a movie studio) provides content to Foster's system for encryption and secure streaming (*e.g.*, via the internet) to a recipient.

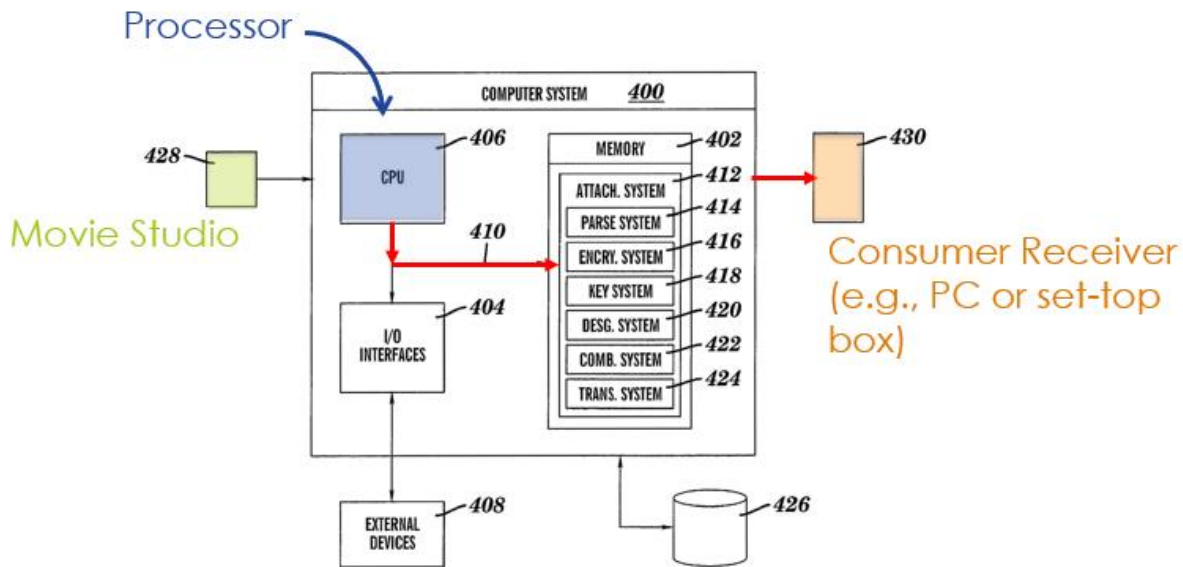


FIG. 16

Ex. 1006 [Foster] Fig. 16 (annotated); [0002] (“a method, system and program product for attaching a title key to encrypted content for synchronized transmission to a recipient.”); [0078] (“computer system 400 is intended to be representative of any system capable of processing content units of an elementary content stream received from source 428, and transmitting the processed content units to a recipient 430.”).

Foster, thus, essentially acts as an encryption middleman for streamed content. Foster, in contrast to the claimed inventions, does not “generate” a plurality of data chunks from a dataset. Rather, it just streams encrypted content in network packets (created in accord with the applicable standards, *e.g.*, MPEG). Nor does Foster’s system even store each chunk on a plurality of different storage devices, as required by the ’116’s independent claims.

Ex. 2003 [Rubin-Decl.] ¶¶ 71-73.

Adding Hayhurst to the combination cannot cure the fundamental difference between Foster and the '116. Thus, unsurprisingly, Petitioner's Foster-Hayhurst ground fails for the multiple reasons below.

B. Petitioner's Proposed Foster-Hayhurst Combination Does Not Disclose The Limitations Of The Independent Claims (All Claims).

1. Foster-Hayhurst Does Not Disclose Or Render Obvious The Preamble Limitation Of The Independent Claims, Under The Parties' Agreed Construction (All Claims).

The preamble limitation of both independent claims states that the claim is directed to “a method for securing a dataset.” The parties have now agreed that a “data set” is “a collection of information *for storage*.” Ex. 2020 [Google-Responsive-Claim-Construction-Brief] 8 n.3. Thus, the preamble limitation requires “a method of securing a collection of information *for storage*.” The preamble limits the claims here because the term “data set,” used in the preamble, is used in the body of the claim. Ex. 1001 ['116] cls. 1 & 9 (“distributing the data set into a plurality of chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set”); *Shoes by Firebug LLC v. Stride Rite Children's Grp., LLC*, 962 F.3d 1362, 1368 (Fed. Cir. 2020) (“use of preamble terms to define positive limitations in the body of claims can evince an inventor's intent that the preamble limit the scope of the claim.”).

Petitioner maps the “data set” solely to Foster’s “content.” Pet., 68-69. But Foster’s definition of “content” makes no mention of “storage.” Ex. 1006 [Foster] [0037] (“Content—any data such as digital image, sound or binary data deliverable from a source to a recipient”). In fact, Foster defines “content” in a way that makes it clear to a POSITA that its content is “for” streaming, *i.e.*, for “deliver[y] from source to recipient,” and therefore **not** for storage.³ Because Petitioner cannot demonstrate that Foster’s “content” is “for storage” it consequently cannot demonstrate that Foster (or the Foster-Hayhurst combination) teaches a method for securing a collection of information for storage, as required by the preamble of the independent claims.

2. Petitioner Fails To Show Foster Discloses “Distributing The Data Set Into A Plurality Of Data Chunks” (All Claims).

Both independent claims require “distributing the data set into a plurality of data chunks.” Ex. 1001 [’116] cls. 1, 9. Petitioner maps the claimed “plurality of data chunks” to Foster’s content units (more specifically, their payloads) or “content packets” and the claimed “data set” to Foster’s “content.” Pet., 68-69.

³ As discussed in the next section (*see* Section IV.B.2), this is important because goes to the heart of why the ’116 and Foster concern fundamentally different, and incompatible, technologies.

Petitioner has not, and cannot, demonstrate that the payloads of Foster’s content packets are “data chunks” and consequently cannot demonstrate that Foster discloses this limitation.

As an initial matter, Petitioner’s assertion that Foster’s “payloads” “are” “data chunks” is entirely unsupported. The Petition simply asserts without explanation that:

These “content packets”/“payloads” 106 are “*a plurality of data chunks*” as claimed because each includes only a portion of digital content 100 (i.e., a subset of the data set), which is all that is required of a data chunk as discussed in §V.B.2 above. Bhattacharjee, ¶256.

Pet., 69; 68 (“Foster’s encryption method, which as illustrated in Foster’s Figure 8 (annotated below), generates a plurality of “payloads” by “parcel[ing]” digital content 100”) (citing Ex. 1005 [Foster] [0064]). As Dr. Rubin explains, however, Petitioner’s alleged evidence does not substantively support this assertion:

Petitioner cites Foster at [0064], but this disclosure simply discloses “parcel[ing]” content into the payloads and does not explain why Foster’s payloads are the claimed “data chunks” (or “shares” when unencrypted). Ex. 1006 [Foster] [0064]. Petitioner’s citation to Dr. Bhattacharjee’s declaration provides no further insight as it merely parrots the Petition. Ex. 1003 [Bhattacharjee-Decl.] ¶ 256.

Ex. 2003 [Rubin-Decl.] ¶ 76. Dr. Bhattacharjee’s conclusory testimony should be afforded little or no weight as it is precisely the sort of conclusory testimony

rejected in *Xerox*. *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential) (“cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight” when “it merely repeats, *verbatim*, the conclusory assertion for which it is offered to support.”); *Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.*, ___ F.4th ___, Case No. 2022-1998, slip op. at *7 n.2 (Fed. Cir. Mar. 27, 2024) (“the conclusory assertions in Dr. Mohazzab’s declaration do not provide substantial evidence for finding a motivation to combine.”)..

In fact, the specifications of Foster and the ’116 indicate to a POSITA that Foster’s “payloads” cannot be the claimed “data chunks.” As Dr. Rubin explains, Foster’s “payloads” are payloads of packets that arise as a result of transmission according to the MPEG video compression standard:

Petitioner and Dr. Bhattacharjee rely on Foster’s “payloads” as the claimed data chunks. Pet., 68-69. Foster teaches that these “payloads” refer to the payloads of MPEG Packetized Elementary Stream (PES) packets (also referred to in Foster as “units”), as illustrated below in Figure 13:

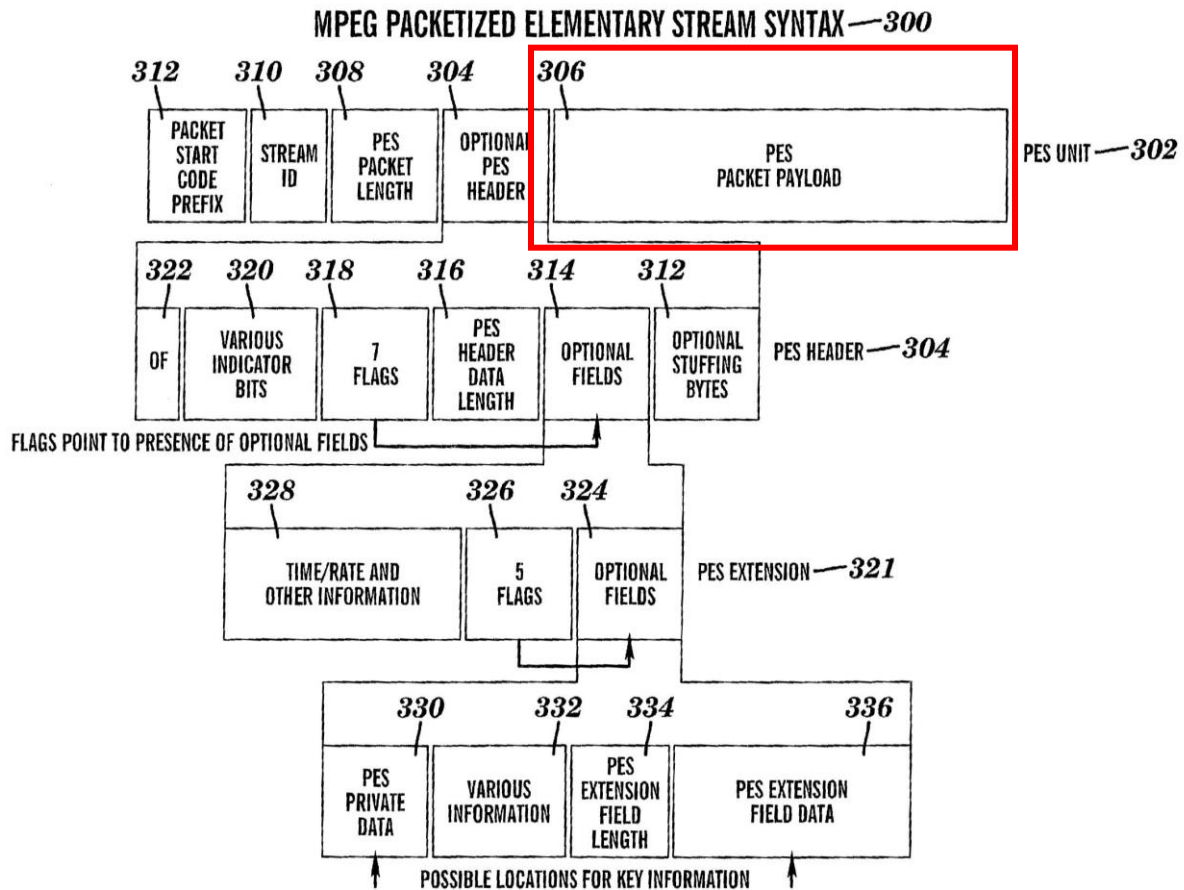


FIG. 13

Ex. 1006 [Foster] Fig. 13, [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”). Foster’s PES packets are also referred to as “data packets.” See Ex. 2011 [Tsai] [0001], cl. 1. Consequently, Petitioner and Dr. Bhattacharjee map the claimed “data chunks” to Foster’s packets (specifically, the payloads of those packets) which are then individually encrypted.

The '116, however, does not refer to data packets as “data chunks.” Indeed, the difference between the '116's data chunks and Foster's data packets goes to the fundamental difference between the '116 and Foster's inventions. As the '116 explains, partitioning the data set into chunks increases security:

Traditional encryption technologies known in the art rely on one or more key used to encrypt the data and render it unusable without the key. ***The data, however, remains whole and intact and subject to attack.*** The secure data parser of the present invention, in one embodiment, ***addresses this problem by performing a cryptographic parsing and splitting of the encrypted file*** into two or more portions or shares, and in another embodiment, preferably four or more shares, adding another layer of encryption to each share of the data, then storing the shares in different physical and/or logical locations. When one or more data shares are physically removed from the system, either by using a removable device, such as a data storage device, or by placing the share under another party's control, ***any possibility of compromise of secured data is effectively removed.***

Ex. 1001 ['116] 57:10-24. Thus, the '116 teaches that its data chunks are “generat[ed]” to secure the data.

By contrast, Foster teaches that its content is “parceled” or “packetized” by virtue of the MPEG packetized elementary stream

standard. Ex. 1006 [Foster] [0072]-[0073]; Ex. 2014 [Overview-of-MPEG-2-Systems] (“An elementary stream is broken up into packets, forming a *packetized elementary stream* (PES).”). These packets allow for transmission of the content. See Ex. 2015 [Newton’s-Telecom-Dictionary] 626 (“**Packet** 1. Generic term for a bundle of data, usually in binary form, organized in a specific way *for transmission*.”); Ex. 2016 [Oxford-Dictionary-of-Computing] 257 (“a group of binary digits forming a message. The group is *transmitted* together”). And that Foster’s packets are for transmission is of no surprise as Foster’s invention “relates to . . . encrypt[ing] content for synchronized transmission to a recipient.” Ex. 1006 [Foster] [0002]. The ’116 data chunks and Foster’s packets serve entirely different purposes.

In other words, by disclosing a method for secure transmission of MPEG data packets, Foster does not disclose “generating a plurality of data chunks” as a POSITA would understand the limitation based on the ’116’s specification. Notably, neither Petitioner nor Dr. Bhattacharjee identify any teaching in the ’116 or in the technical literature suggesting that a data packet would qualify as a “data chunk.”

Ex. 2003 [Rubin-Decl.] ¶¶ 78-81.

Thus, Petitioner fails to demonstrate that Foster (or the Foster-Hayhurst combination) discloses or renders obvious “distributing the data set into a plurality of data chunks.”

3. Foster Does Not Disclose Or Render Obvious “Separately Storing Each Data Chunk Of The Plurality Of Data Chunks . . . On A Plurality Of Different Storage Devices” (All Claims).

The claims require “*separately storing each data chunk of the plurality of data chunks* together with one of the plurality of [obfuscated/transformed] different encryption keys *on a plurality of different storage devices.*” Ex. 1001 [’116] cls. 1, 9. Even assuming, *arguendo*, that the data packets of Foster could correspond to the claimed chunks, this limitation is not satisfied by Foster because Foster does not store its data packets on *storage devices*, as required by claim 1. In Foster, data is streamed to a “receiver” for immediate decoding and play on a playback device such as a set top box, not for secure long-term storage. As previously explained, this distinction goes to the fundamental difference between the ’116’s inventions—for secure storage of data—and Foster’s invention—for streaming content from a content owner to a consumer. See Section IV.A.

Petitioner argues that Foster discloses that “the ‘processed content unit 116’ . . . is stored by the content provider or transmitted to a receiver (e.g., a set-top box)” and that in the Foster-Hayhurst combination, “each encrypted content unit (i.e., ‘processed content unit 116’) is stored on a different Foster-Hayhurst subscriber unit” which is essentially a “conventional set-top box.” Pet., 72-73. Petitioner’s argument, however, fails because Foster’s “receiver” is not and does not include a claimed “storage device.”

Although Petitioner never explains what a “storage device” is or clearly maps what the “plurality of different storage devices” is in its combination, Petitioner asserts that Foster’s “receiver” and the Foster-Hayhurst set-top box store processed content units. Petitioner’s argument thus rests upon the unsubstantiated premise that any device that has a memory is a claimed “storage device.” This is wrong, as Dr. Rubin explains:

The ’116 is directed toward “securing data from unauthorized access or use.” Ex. 1001 [’116] 1:23-24. As such, an important aspect of the ’116’s invention is securely storing data. *Id.*, 61:67-62:4 (“One advantage is the security gained from moving shares of the data to different locations on one or more data depositories or storage devices, that may be in different logical, physical or geographical locations.”); *see generally id.*, 2:39-6:60 (all embodiments in summary of invention include storing data in storage facilities or storage media). The ’116 gives some examples of “suitable” storage devices:

...one or more portions are stored on ***a smart card, a government Common Access Card, any suitable physical storage device (e.g., magnetic or optical disk, USB key drive, etc.)***, or any other suitable device.

Id., 67:36-40; *see also id.*, 57:20-24 (“When one or more data shares are physically removed from the system, either by using a removable device, such as a data storage device, or by placing the share under another party’s control, any possibility of compromise of secured data

is effectively removed.”). Thus, the ’116 provides specific examples of what is meant by a “storage device,” *i.e.*, “magnetic or optical disk, USB key drive, etc.” Each of these examples of a “storage device” is one that is primarily dedicated to long-term storage and not merely a device that has a memory for transiently storing data packets as they arrive for processing and display.

Foster teaches that its receiver, by contrast, is merely a PC, DVD player or, in Petitioner’s example, a consumer set-top box. Pet., 72 (“receiver (*e.g.*, consumer set-top box)”); Ex. 1006 [Foster] [0040] (“Receiver-***a consumer device, such as a set-top box, a DVD player, etc.***, that receives content directly from a content owner, from a content service or from another receiver within a consumer home network.”); [0048] (a “PC” uses prior-art Digital Rights Management System). While a PC, DVD player, or set-top box may be capable of storing data, none of these devices are “storage devices” as that term is used in the ’116. Rather, they are used to read and immediately play content. Any “storage” of the data in short-term memory is simply to allow the data packet to be unpacked so the stream can be played. Ex. 2021 [Cambridge-Dictionary] (defining set-top box as “an electronic device that makes it possible to watch digital broadcasts on ordinary televisions”); *cf.* Ex. 2019 [Microsoft-Computer-Dictionary] 90 (“CD player *n.* ...A device that reads the information stored on a CD.”). Indeed, Foster does not even require that “receivers” be capable of storing data but simply that they “receive[] content directly from a content owner.” Ex. 1006 [Foster] [0040]. Thus, a POSITA would not understand Foster’s “receiver” as a device primarily dedicated to long-

term storage, and thus would not understand Foster to teach “storing” data chunks on a plurality of different “storage devices.”

Ex. 2003 [Rubin-Decl.] ¶¶ 86-87.

Thus, a POSITA reviewing the ’116 patent would not understand a “storage device” to encompass something like Foster’s receiver (*e.g.*, a set-top box or a DVD player) because the examples of storage devices given in the ’116—“magnetic or optical disk, USB key drive, etc.”—are each devices primarily dedicated to long-term storage. While the ’116 does use the word “etc.,” that just refers to things of a similar type. *IBM v. Iancu*, 759 Fed. App’x. 1002, 1007–08 (Fed. Cir. 2019) (the word “etc.” “indicate[s] that only things of a type similar to the itemized ones are covered . . . [w]e have recognized that . . . ‘etc.’ sometimes have just that meaning.”) (citing *Archer Daniels Midland Co. v. United States*, 561 F.3d 1308, 1313 (Fed. Cir. 2009) (holding that the “rule of ejusdem generis . . . limits the additional [things] included by the general phrase ‘etc.’ to others of the types listed”)). Consequently, Petitioner fails to show that the Foster-Hayhurst combination discloses “separately storing each data chunk of the plurality of data chunks . . . on a plurality of different storage devices” because, *inter alia*, it does not disclose storing anything on a storage device, as the term is used in the ’116. The inventions claimed in the ’116 patent are fundamentally different.

V. CONCLUSION

Thus, Petitioner fails to demonstrate a reasonable likelihood of success as to any of the challenged claims, and the Petition should be denied.

Respectfully submitted,

/ Stephen J. Elliott /

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

SULLIVAN & CROMWELL LLP

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

Nathan Lowenstein, *pro hac vice* to be filed

Colette Woo, *pro hac vice* to be filed

LOWENSTEIN & WEATHERWAX LLP

Date: March 28, 2024

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Preliminary Response (the “POPR”) consists of 8,130 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The POPR 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).

Respectfully submitted,

/ Colette Woo /

Date: March 28, 2024

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 PRELIMINARY RESPONSE

EXHIBITS 2003, 2005-2011, 2014-2016, 2019-2021, 2023-2027

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

Elisabeth H. Hunt
Richard F. Giunta
Marc S. Johannes

EHunt-PTAB@wolfgreenfield.com
RGiunta-PTAB@wolfgreenfield.com
MJohannes-PTAB@wolfgreenfield.com

Respectfully submitted,

/ Colette Woo /

Date: March 28, 2024