Trials@uspto.gov
571-272-7822

Paper 42
Entered: May 16, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

IPR2024-00212
Patent 11,178,116 B2

Before THOMAS L. GIANNETTI, JASON M. REPKO, and STEPHEN E. BELISLE, *Administrative Patent Judges.*

GIANNETTI, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background

Google LLC ("Petitioner") filed a Petition requesting *inter partes* review of claims 1–3 and 5–14 of U.S. Patent No. 11,178,116 B2 (Ex. 1001, "the '116 patent"). Paper 2 ("Pet."). Security First Innovations, LLC ("Patent Owner") filed a Preliminary Response. Paper 10 ("Prelim. Resp.").

We determined that Petitioner established a reasonable likelihood that it would prevail with respect to at least one claim challenged in the Petition. Paper 11 ("Institution Dec."). We therefore instituted *inter partes* review as to all of the challenged claims of the '116 patent and all of the asserted grounds of unpatentability. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1356 (2018); 37 C.F.R. § 42.108 (a) ("When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.").

Following institution of the trial, Patent Owner filed a Response (Paper 17, "PO Resp."), Petitioner filed a Reply (Paper 21, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 29, "PO Sur-reply").

A consolidated oral hearing with IPR2024-00214 and IPR2024-00215 was held on February 27, 2025. A transcript of the hearing is part of the record. Paper 41 ("Hearing Tr.").

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision issued pursuant to 35 U.S.C. § 318(a). For the reasons we discuss below, we determine that Petitioner has proved by a preponderance of the evidence that claims 1, 2, 5, 9, and 11–14 of the '116 patent are unpatentable.

B. Related Matters

According to the parties, the ’116 patent has been asserted in *Security First Innovations, LLC v. Google LLC*, No. 2:23-cv-00097 (E.D. Va.). Paper 4, 1; Paper 9, 1. The parties further indicate that IPR2024-00213, IPR2024-00214, and IPR2024-00215 are related matters. Paper 4, 1.

C. Real Parties-in-Interest

Petitioner identifies Google LLC as the real party-in-interest. Pet. xi. Patent Owner identifies Security First Innovations, LLC, as the real party-in-interest. Paper 4, 1,

D. The ’116 Patent

The ’116 patent generally relates to securing data from unauthorized access or use. Ex. 1001, 1:21–22. The data to be secured is parsed, split, or separated into several parts. *Id.* at 2:41–43. The data is encrypted, either before or after the parsing, splitting, or separating. *Id.* at 2:43–46. The encryption step can be repeated. *Id.* at 2:46–48. According to the ’116 patent, a secure data processor performs a cryptographic parsing and splitting of the encrypted file into two or more portions or shares, preferably four or more shares. *Id.* at 57:13–17. This adds another layer of encryption to each share of the data. *Id.* at 57:18. Then storing the shares in different physical and/or logical locations, either by using a removable device, such as a data storage device, or by placing the share under another party’s control, effectively removes “any possibility of compromise of secured data.” *Id.* at 57:19–24.

Figure 21, reproduced below, illustrates one embodiment of the ’116 patent.

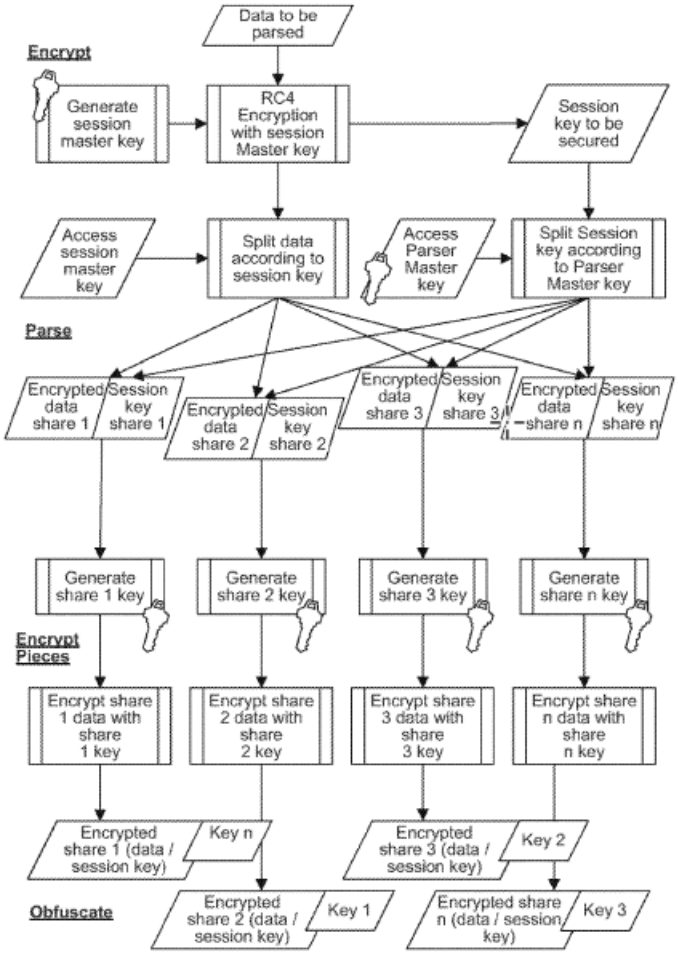


FIG. 21

Figure 21 illustrates a process for parsing, splitting, and separating data with encryption and storage of the encryption master key with the data. Ex. 1001, 7:56–58. As shown in Figure 21, the steps of the exemplary process performed by the secure data parser on data to store the session master key with the parsed data are:

> 1. Generating a session master key and encrypting the data.
>
> 2. Separating the resulting encrypted data into four shares or portions of parsed data according to the pattern of the session master key.
>
> 3. Storing the session master key along with the secured data shares in a data depository.

> 4. Separating the session master key according to the pattern of the Parser Master Key and appending the key data to the encrypted parsed data. The resulting four shares of data will contain encrypted portions of the original data and portions of the session master key.
>
> 5. Generating a stream cipher key for each of the four data shares.
>
> 6. Encrypting each share, then storing the encryption keys in different locations from the encrypted data portions or shares: Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.

Id. at 57:41–62. To restore the original data format, the steps are reversed. *Id.* at 57:63.

E. Claims

Of the challenged claims, claims 1 and 9 are independent. Claim 1 follows:

> 1. [PRE] A method for securing a data set, the method comprising:
>
> [1A] distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set;
>
> [1B] encrypting each of the data chunks with a respective one of a plurality of encryption keys;
>
> [1C] obfuscating each of the plurality of different encryption keys; and
>
> [1D] separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.

Ex. 1001, 100:19–31.[1]

---

[1] Paragraph identifiers in brackets have been added in the same manner as used in the Petition. *See* Pet. 82–83 (claim listing).

Claim 9 substitutes "transforming" and "transformed" for "obfuscating" and "obfuscated" in limitations 1C and 1D, respectively, but is otherwise identical to claim 1. *Id.* at 100:61–101:6.

F. References and Other Evidence

Petitioner relies on the following:

Name	Reference	Exhibit No.
Tajima	US 2003/0028493 A1, published Feb. 6, 2003	1005
Foster	US 2003/0200176 A1, published Oct. 23, 2003	1006
Hayhurst	WO2004/008289, published Jan 22, 2004	1007
Shyu	US 6,021,391, issued Feb. 1, 2000	1016
Rivest	Ronald J. Rivest, *All-or-Nothing Encryption and the Package Transform*, Fast Software Encryption, 4th Intl. Workshop, FSE'97, Jan. 20–22, 1997 Proceedings, pp. 210–218.	1034

In addition, Petitioner submits the Declaration of Samrat Bhattacharjee, Ph.D. Ex. 1003 ("Bhattacharjee I Decl."). Petitioner relies also on a Reply Declaration of Dr. Bhattacharjee. Ex. 1111 ("Bhattacharjee II Decl."). Patent Owner submits a first Declaration of Aviel D. Rubin, Ph.D. Ex. 2003 ("Rubin I Decl.") and a Second Declaration of Dr. Rubin ("Rubin II Decl.") Ex. 2033. In addition, the parties have submitted deposition transcripts for Dr. Bhattacharjee and Dr. Rubin.[2]

G. Petitioner's Reply Declaration

Patent Owner argues that Petitioner has submitted "a 118-page, 25,000-word Reply declaration, comprising 201 paragraphs of additional testimony and 42 new exhibits." PO Sur-reply 1 (emphasis omitted). Patent Owner argues that "[t]his new evidence, in support of new arguments,

[2] Exhibit 1099 ("Rubin Dep."); Exhibit 2034 ("Bhattacharjee I Dep."); Exhibit 2046 ("Bhattacharjee II Dep.").

should not be considered." *Id.* We agree with Patent Owner that the length of Dr. Bhattacharjee's 118-page Reply Declaration is excessive. However, we are not persuaded to give the declaration "no weight," especially in view of the fact that our rules place no page limit on declarations and Petitioner has not placed before us a motion to strike the declaration. We consider also the fact that Patent Owner itself submitted over 70 pages of declaration testimony by Dr. Rubin. *See* Ex. 2003, Ex. 2033.

On the other hand, our rules do prohibit incorporating documents by reference. *See* 37 C.F.R. § 42.6(a)(3). Our PTAB Consolidated Trial Practice Guide (Nov. 2019) ("Trial Practice Guide")[3] provides guidance on incorporation by reference: "[P]arties that incorporate expert testimony by reference in their petitions, motions, or replies without providing explanation of such testimony risk having the testimony not considered by the Board." *Id.* at 35–36. The Practice Guide further explains: "Expert testimony may be presented to establish the scope and content of the prior art for determining obviousness and anticipation. . . . Expert testimony, however, cannot take the place of a disclosure in a prior art reference, when that disclosure is required as part of the unpatentability analysis." *Id.* at 36.

Consistent with this guidance, we will focus our analysis on arguments presented in the briefing of the parties and their support. We will not address arguments in either party's declarations that are not discussed in the briefs or arguments that are incorporated by reference from the expert declarations. Nor will we give weight to expert testimony that attempts to fill gaps in the prior art presented in the Petition with new evidence. *See* Trial Practice Guide at 74–75.

---

[3] Available at https://www.uspto.gov/TrialPracticeGuideConsolidated.

H. Asserted Grounds

Petitioner asserts that claims 1–3 and 5–14 are unpatentable on the following grounds. Pet. 1.

Claims Challenged	Pre-AIA[4] 35 U.S.C. §	Reference(s)/Basis
1, 5–8	102/103	Tajima
1, 2, 9, 11–14	103	Tajima, Foster
9–14	103	Tajima, Rivest
1–3, 6	103	Tajima, Rivest, Shyu
1, 2, 5, 9, 11	103	Foster, Hayhurst

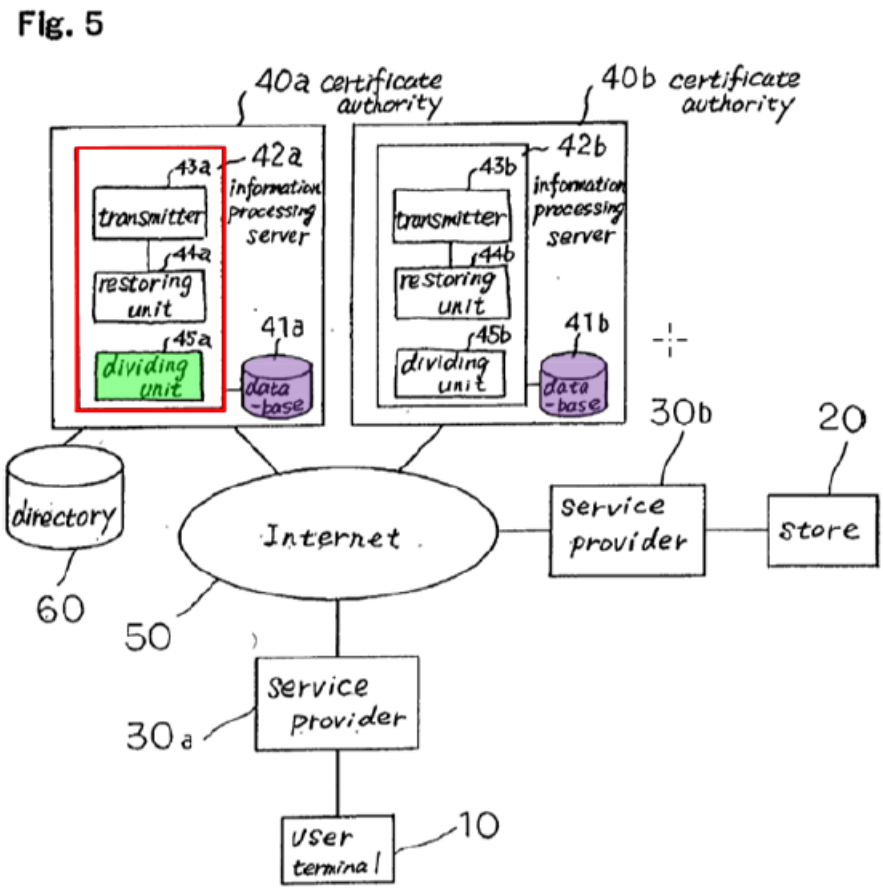
I. Overview of the Principal Prior Art Asserted

1. Tajima

Tajima discloses "a personal information management system and a personal information management method for managing personal information by means of areas that are connectible to the Internet." Ex. 1005 ¶ 2. Personal information that is registered with areas that can be connected to the Internet is divided into a plurality of data portions. *Id.* at code (57). These data portions are then each registered with areas that are under different control. *Id.* When a request to acquire this personal information is subsequently issued, the data portions that are registered with areas under different control are combined to restore the personal information. *Id.*

[4] For purposes of this Decision, we assume the claims at issue have an effective filing date prior to March 16, 2013, the effective date of the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"). *See* Ex. 1001, code (60). We therefore apply the pre-AIA versions of 35 U.S.C. §§ 102 and 103.

Tajima's Figure 5, annotated by Petitioner, is reproduced below. Pet. 9.

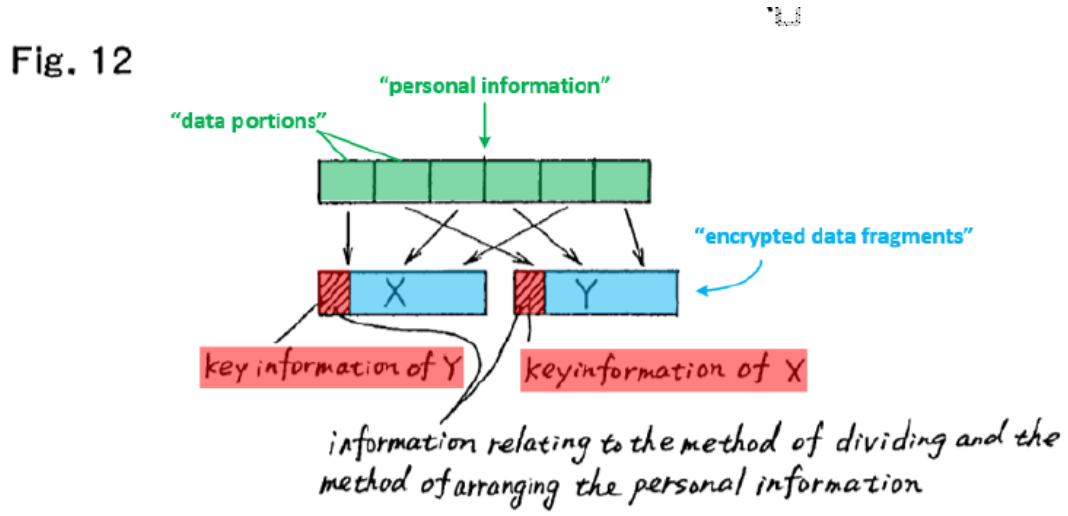


As shown in annotated Figure 5, this embodiment of Tajima is made up of user terminal 10 that is connectible to Internet 50; service provider 30a to which user terminal 10 subscribes for handling connections of user terminal 10 to Internet 50; certificate authority 40a for both certifying personal information relating to the user of user terminal 10 and registering a portion of the personal information relating to the user of user terminal 10; and directory 60 for registering a public key that the user of user terminal 10 has registered with certificate authority 40a in advance. Ex. 1005 ¶ 67. In addition, certificate authority 40a includes information processing server 42 made up of dividing unit 45a (in green) for dividing the personal information

relating to the user of user terminal 10 and registering a portion of this information with database 41a (in purple). Certificate authority 40b has a similar configuration. *Id.*

In operation, personal information submitted by the user of terminal 10 to certificate authority 40a is first divided into a plurality of data portions, each of a predetermined fixed length. Ex. 1005 ¶ 101. This plurality of data portions is then arranged as two data fragments, data fragment X and data fragment Y, according to a set method of arranging. *Id.* Data fragment X is then registered with database 41a of certificate authority 40a, and data fragment Y is registered with database 41b of certificate authority 40b. *Id.*

Annotated Figure 12, reproduced below, illustrates data fragments X and Y. Pet. 11.



In annotated Figure 12, data fragments X and Y are shown in blue. Ex. 1005 ¶ 111. Each fragment is encrypted, and encrypted data fragment X is then registered with database 41a of certificate authority 40a and encrypted data fragment Y is registered with database 41b of certificate authority 40b. *Id.* Information regarding the key that was used for the encryption of data

fragment Y (in red) is attached to encrypted data fragment X, and information regarding the key that was used in the encryption of data fragment X (also in red) is attached to encrypted data fragment Y. *Id.*

2. Foster

Foster discloses encrypting streaming content before transmitting it to a recipient. Ex. 1006 ¶ 2. Foster's Figure 8 is reproduced below with Petitioner's annotations. Pet. 51.

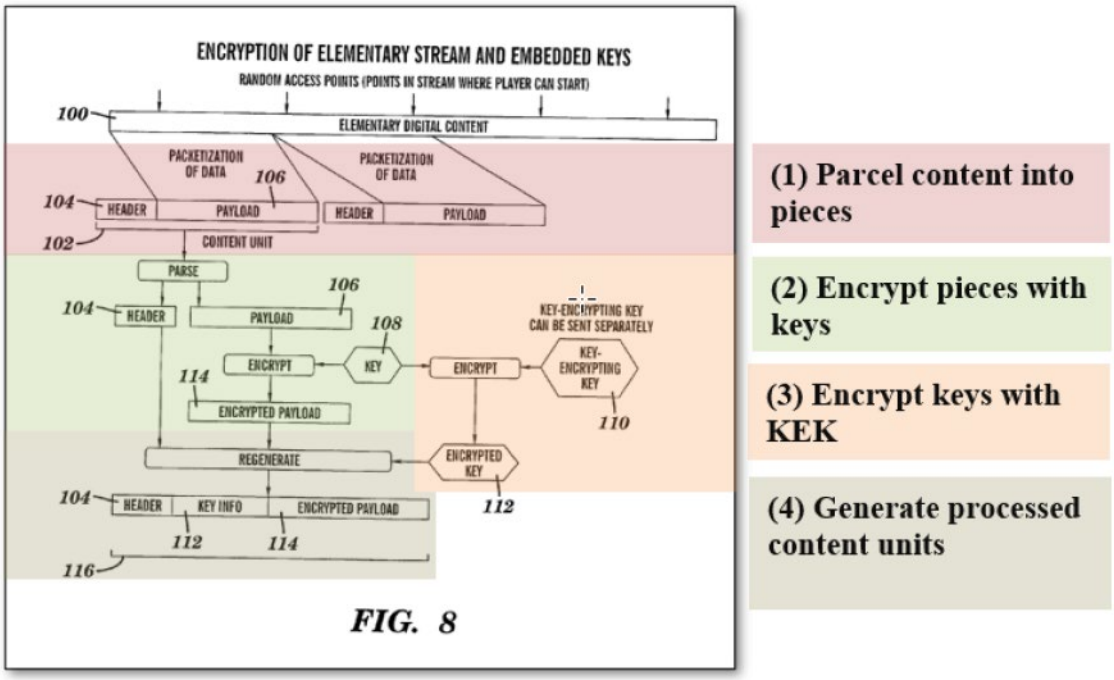


Figure 8 is annotated by Petitioner with labels for four different parts of Foster's method: (1) parceling digital content 100 into content units 102 containing header 104 and payload 106, (2) encrypting payload 106 with title key 108 to yield content package 114, (3) encrypting each key 108 with key-encrypting key (KEK) 110 to create encrypted key 112, and (4) combining encrypted key 112, encrypted content package 114, and header 104 as processed content unit 116 that can be transmitted to a recipient and stored. *Id.*; *see also* Ex. 1006 ¶ 64.

3. *Hayhurst*

Hayhurst relates to securely handling and storing electronic media, such as video-on-demand. Ex. 1007 ¶¶ 2, 8. Hayhurst's system segments the media for distribution to subscriber units for storage. *Id.* ¶ 6. When a subscriber unit requests a media file, the main server instructs the network subscribers to forward copies of the segments stored in those units to the requesting subscriber. *Id.* ¶ 7. The subscriber units encrypt the file segments before forwarding them to the requesting subscriber. *Id.* A main server then provides an encryption key to the requesting subscriber to unlock the media file. *Id.* According to Hayhurst, this method deters piracy because no single subscriber unit has more than a segment of the media file. *Id.* ¶ 8.

Hayhurst's Figure 1, reproduced below, illustrates this operation.

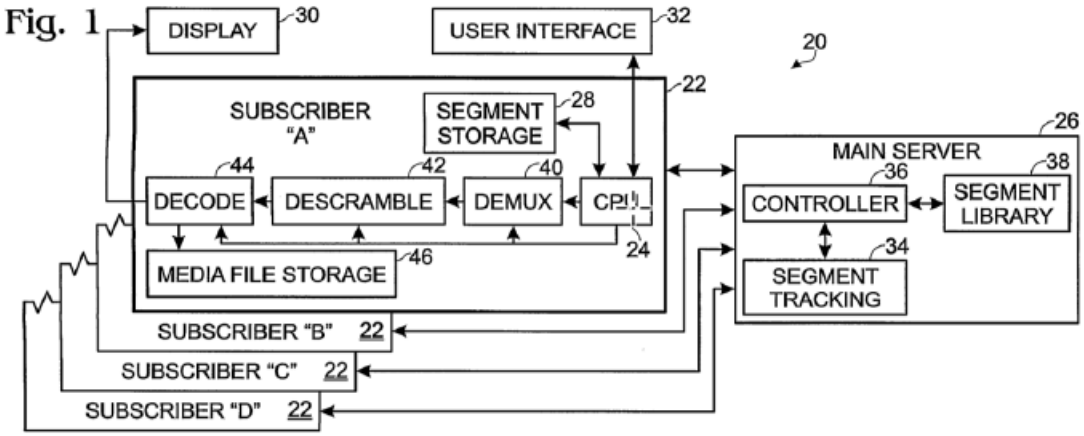


Figure 1 is a block diagram of Hayhurst's system for decentralized media delivery. Ex. 1007 ¶ 12. Each subscriber unit 22 includes storage device 28, such as a conventional hard disk. *Id.* ¶ 18. This storage device stores segments of one or more media files (e.g., movies). *Id.* In Figure 1, each unit 22 receives from main server 26 one or more segments of a complete media file. *Id.* ¶ 20. The segments are stored in the corresponding segment

storage 28. *Id.* Each segment is part of a different movie. *Id.* When the main server receives a movie request from a requesting subscriber, the server instructs the network subscriber units to direct all of the stored segments for the requested movie to the requesting subscriber. *Id.* ¶ 28.

II. ANALYSIS OF THE CHALLENGED CLAIMS

A. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art "would have had at least a bachelor's degree in computer science, computer engineering, or a related field, with three years of experience in the area of securing data from unauthorized access or use." Pet. 4 (citing Bhattacharjee Decl. ¶¶ 41–45). Petitioner further asserts that a "higher level of education may substitute for less experience." *Id.*

At the institution stage, Patent Owner did not oppose Petitioner's assertions or provide a definition of a person of ordinary skill in the art. *See generally* Prelim. Resp.; Rubin I Decl. ¶ 20 (accepting Dr. Bhattacharjee's proposed qualifications for the purposes of his declaration). We regarded Petitioner's description as consistent with the prior art before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). Thus, for the purpose of our Institution Decision, we adopted Petitioner's proposal. Institution Dec. 11.

Post-institution, neither party has contested this description. *See* Rubin II Decl. ¶ 20 (accepting Dr. Bhattacharjee's definition). For the reasons given, we maintain our previous description of the person of ordinary skill.

B. Claim Construction

In *inter partes* reviews, the Board interprets claim language using the same standard used in district courts, as described in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b) (2023). Under this standard, claim terms have their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art at the time of the invention, in light of the language of the claims, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1313–14.

"The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'" *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Pre-institution, neither party explicitly proposed constructions for disputed claim terms. Petitioner acknowledged the existence of "competing proposed constructions" in the parallel district court action. Pet. 7 (citing Ex. 1042, 1043). But Petitioner contended that "this Petition presents alternative mappings of the prior-art disclosures to both parties' proposed constructions of disputed terms, thus demonstrating unpatentability regardless of which proposed construction is correct." *Id.*

Patent Owner's Preliminary Response did not address directly claim construction (although it does contend that the cited prior art does not teach or suggest various limitations of the challenged claims as construed by Petitioner). *See, e.g.,* PO Resp. 2–3 (relating to disclosure of a key in Tajima); *see also* discussion in Section II.C, *infra*.

Notwithstanding the absence of any explicit claim construction proposals from the parties, and after reviewing the parties' submissions, the Board provided guidance in the Institution Decision on the term "storage devices" in claims 1 and 9. *See* Institution Dec. 12 (commenting that we did not see support for limiting the term "storage devices" to "long-term storage"). However, we decided that we did not need to decide whether the claims require long-term storage to resolve a controversy. *Id.*; *see Vivid Techs.*, 200 F.3d at 803. Post-institution, this construction does not appear to be at issue, and therefore, we do not address it in this Decision.

We do not see the need for any further claim constructions for this Decision, and therefore we construe the claims in accordance with their plain meaning. *See Phillips*, 415 F.3d at 1313–14.

C. Tajima Grounds

1. Introduction

Petitioner asserts four separate grounds based on Tajima. *See* Pet. 1. For each of these grounds, Petitioner provides an element-by-element analysis, supported by testimony from Dr. Bhattacharjee. Pet. 8–51; Bhattacharjee I Decl. ¶¶ 59–211.

2. Tajima Alone

Petitioner challenges claims 1 and 5–8 based on Tajima alone. Pet. 13–33. Petitioner contends that Tajima anticipates claims 1 and 5–8 and, alternatively, that those claims would have been obvious in light of Tajima. *Id.*

Focusing on claim 1, Petitioner identifies Tajima's data fragments as the "data chunks" recited in claim limitation 1[A]. Pet. 15–17. Petitioner explains that "Tajima forms multiple data fragments ([1A]'s '*plurality of data chunks*') by dividing personal information (the claimed '*data set*' in the

Fig. 12 embodiment) or by dividing encrypted personal information (the claimed '*data set*' in the Fig. 13 embodiment) into 'a plurality of data portions' of 'fixed' or 'arbitrary length' that are 'then arranged into two data fragments, data fragment X and data fragment Y, according to a set method of arrangement.'" *Id.* at 15–16 (citing Ex. 1005 ¶¶ 111, 113); *see also* Bhattacharjee I Decl. ¶¶ 84–86.

Petitioner next addresses the "encryption key" recitations in claim 1. Pet. 18–19. Claim limitation 1[B] calls for "encrypting each of the data chunks with a respective one of a plurality of encryption keys." *Id.* at 18. Petitioner contends that "Tajima meets [1B] because in both the Fig. 12 and Fig. 13 embodiments 'data fragment X and data fragment Y are each *encrypted*' using a different key, and each key is then stored with a data fragment that key did not encrypt, as illustrated in Figs. 12 and 13." *Id.* Claim limitation 1[C] calls for "obfuscating each of the plurality of different encryption keys." *Id.* at 19. Petitioner contends "Tajima meets [1C] because 'key information of Y' is attached to encrypted data fragment X and 'key information of X' is attached to encrypted data fragment Y, in the Fig. 12 and 13 embodiments." *Id.* Claim limitation 1[D] calls for "separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices." *Id.* at 23. Petitioner contends "Tajima's attaching key information to encrypted data that it did not encrypt and registering the resulting data fragments on respective different databases meets [1D]." *Id.* Thus, in each of these instances, Petitioner identifies Tajima's "key information" with the encryption key recited in the claims.

Patent Owner responds that "[i]n 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." PO Resp. 1 (citing Pet. 20–22, 24). Patent Owner continues, "[h]owever, Tajima does not state or suggest that the key itself is encompassed by 'information regarding the key,' and what Tajima does disclos[e] indicates it is not." *Id.* at 2 (citing Tajima's Fig. 12, reproduced in Section I.I.1, *supra*).

We agree with Patent Owner that Petitioner fails to prove that Tajima discloses storing a key with each data fragment.[5] Tajima's description of Figure 12 is unambiguous in its description of storing "key information" (not encryption keys) with the fragments:

> 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.

Ex. 1005 ¶ 0111. Dr. Rubin testifies, succinctly, that "I do not believe that a [person of ordinary skill] 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.'" Rubin II Decl. ¶ 41. He further testifies that "[w]hen Tajima wishes to refer to a 'key,' it does so directly" (citing many instances where Tajima makes explicit reference to keys). *Id.* ¶ 42 (citing Ex. 1005 ¶¶ 67, 70, 71, 75, 77, 86, 88, 89). We find Dr. Rubin's reasoning on this issue persuasive.

On the other hand, we find Dr. Bhattacharjee's response less convincing. Bhattacharjee II Decl. ¶¶ 5–23. We find that he does not

[5] Petitioner states that it does not rely on the doctrine of inherency to establish that this limitation is met by Tajima. Pet. Reply 2.

adequately support his opinion that a person of ordinary skill would understand that Tajima uses the terms "information regarding the key" and "key information" to refer to an encryption key. *Id.* ¶ 5 (citing Bhattacharjee I Decl. ¶ 103, 131). Lacking support for disclosure of an encryption key in Tajima itself, Dr. Bhattacharjee turns to other references, including Foster. *Id.* ¶¶ 7–9. Dr. Bhattacharjee testifies that "Foster's use of the term 'key information' to describe information that includes the key and additional information . . . explains why Tajima did not just say 'key' when referring to the information attached to the data fragments." *Id.* ¶ 8. Dr. Bhattacharjee's testimony is unconvincing. In Foster, there is explicit disclosure of including the encrypted title key itself in the header extension. Ex. 1006 ¶ 66 ("As depicted, header extension 118 includes encrypted title key 112 . . . "). In contrast, Dr. Bhattacharjee cites no similar disclosure in Tajima. In fact, Dr. Bhattacharjee's reliance on other references to support anticipation runs contrary to the rule that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in *a single prior art reference*." *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987) (emphasis added). We do not find Dr. Bhattacharjee's testimony based on Foster and other references convincing of anticipation by Tajima.

Nor do we find Petitioner's alternative obviousness challenge based on Tajima persuasive. Pet. 22. The Petition includes a single-sentence explanation of this obviousness contention: "Even 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." *Id.* (citing

Bhattacharjee I Decl. ¶ 104). The cited testimony from Dr. Bhattacharjee at paragraph 104 of his initial declaration mirrors the Petition and provides no record citations to support his opinion of obviousness. Such unsupported expert testimony is entitled to little weight. "Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight." 37 C.F.R. § 42.65(a); PTAB Consolidated Trial Practice Guide 40 (Nov. 2019) ("Trial Practice Guide") ("Opinions expressed without disclosing the underlying facts or data may be given little or no weight.").[6]

In contrast, Dr. Rubin testifies in detail concerning the weaknesses in Petitioner's alternative obviousness ground. Rubin I Decl. ¶¶ 62–69; Rubin Dep. 176:16–180:7. As Dr. Rubin explains, "I see no evidence or explanation in either the Petition or Dr. Bhattacharjee's declaration of why attaching the encryption key itself to a data fragment 'would have been an obvious and conventional way' to modify Tajima." Rubin I Decl. ¶ 63. He explains that "Tajima's method of attaching 'information regarding the key,' rather than the key itself, has the security benefit that an attacker with all of Tajima's data fragments still would not possess all the plaintext keys." *Id.* ¶ 67.

Petitioner's Reply repeats its reliance on "other prior-art references," including Foster. Pet. Reply 4–6, 9–11. For the reasons previously given, we find that this argument is without merit. Furthermore, we are not persuaded by Petitioner's argument based on certain claims of Tajima reciting an encryption key. Pet. 21–22; Pet. Reply 6–7. As Patent Owner points out, those claims are directed to another embodiment (Figure 11) that

[6] Available at https://www.uspto.gov/TrialPracticeGuideConsolidated.

does not disclose encrypting data fragments, and therefore does not address storing encryption keys. PO Resp. 5. Patent Owner explains further that "Petitioner does not rely on Tajima's Figure 11 embodiment." *Id.*

For the reasons given, we find that Petitioner has failed to prove by a preponderance of the evidence that claim 1 of the '116 patent is anticipated by Tajima or that claim 1 would have been obvious in light of Tajima alone. Claims 5–8 depend from claim 1 and therefore incorporate the limitations of claim 1 including reciting an encryption key. For the reasons given for claim 1, we find that Petitioner has failed to prove by a preponderance of the evidence that those claims of the '116 patent are anticipated by Tajima or that they would have been obvious in light of Tajima alone.

3. Tajima and Foster

In the second of its four Tajima grounds, Petitioner contends that claims 1, 2, 9, and 11–14 would have been obvious in light of Tajima and Foster. Pet. 33–46; Bhattacharjee I Decl. ¶¶ 139–179. Petitioner contends that each limitation of claim 1 is met by the Tajima-Foster combination. *See* Pet. 40–42. Dr. Bhattacharjee provides supporting testimony. Bhattacharjee I Decl. ¶¶ 164–167. Petitioner provides a similar analysis for claim 9 and the dependent claims 2 and 11–14. Pet. 42–46; Bhattacharjee I Decl. ¶¶ 168– 179. Petitioner relies on Foster for its teaching of key encryption using a KEK (Key Encryption Key). Pet. 34–37. Petitioner asserts that a person of ordinary skill would have combined Tajima's techniques of dividing personal information and securely storing data fragments on databases under separate control with Foster's key-encryption technique with a reasonable expectation of success. Pet. 37–40; Bhattacharjee I Decl. ¶155–163. Petitioner argues that there is a well–known security risk in storing unencrypted keys. Pet. 33–34 (citing Bhattacharjee I Decl. ¶¶ 141–

143). Dr. Bhattacharjee testifies that there would have been numerous benefits in encrypting Tajima's keys, among them increased security of a user's personal information. Bhattacharjee I Decl. ¶¶ 154–159.

Patent Owner responds that Petitioner "fails to demonstrate" a motivation to combine the references. PO Resp. 9. Patent Owner argues that "Tajima and Foster are directed to entirely different fields and to different problems." *Id*. We disagree. As Petitioner points out, both Tajima and Foster are in the field of securing data, as is the '116 patent. Pet. Reply 13–14 (citing Ex. 1005 ¶ 44; Ex. 1006 ¶ 3). Dr. Bhattacharjee testifies, "Tajima and Foster also both describe techniques for securing data using encryption and securely storing keys with encrypted data." Bhattacharjee II Decl. ¶ 35 (citing Ex. 1005 ¶¶ 109–114; Ex. 1006 ¶¶ 64–71). Patent Owner argues Foster's disclosure of a KEK would have been "redundant" to Tajima's key-securing obfuscation technique. PO Resp. 18. We find this argument is unavailing. As Petitioner points out, Patent Owner's argument "ignores Tajima's vulnerability that Foster's key-encryption addresses." Pet. Reply 16. More specifically, "[r]equiring an attacker to obtain KEKs to decrypt Tajima's encryption keys in addition to de-obfuscating them is not 'redundant' to only having to de-obfuscate them." Pet. Reply 16 (emphasis omitted) (citing Bhattacharjee II Decl. ¶¶ 41–44). We find that Petitioner's argument for combining the references is persuasive for the reasons given.

Patent Owner further argues that Tajima and Foster address different problems and disclose solutions that are "fundamentally at odds." PO Resp. 9–16, 25–27. Patent Owner asserts that "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." *Id.* at 15 (emphasis omitted). Patent Owner

continues, "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.* (alterations in original) (citing Ex. 1006 ¶ 7). We are not persuaded by this argument. As noted *supra*, for the reasons given, we find that both Tajima and Foster are in the field of securing data from unauthorized access. Pet. Reply 13. Furthermore, as Petitioner points out, we find that in Petitioner's combination of Tajima and Foster, Tajima's data (which does not require synchronization) is secured, not Foster's. *See* Pet. 34–36 (providing reasons for encrypting Tajima's keys); Pet. Reply 17–18 ("Synchronization of Foster's data is irrelevant to Tajima-Foster because Tajima-Foster does not restore Foster's data."). Thus, we find that Patent Owner's argument based on the need to synchronize Foster's data for streaming is unavailing.

We have considered Patent Owner's other arguments and find them lacking. *See, e.g.*, Patent Owner's Sur-reply, which repeats the arguments that Tajima and Foster are in a "different field," "fundamentally at odds," "[i]n direct contrast," and that applying Foster's KEK teachings to Tajima would be "redundant." PO Sur-reply 2–9. For reasons already discussed, we find these arguments unconvincing.

In sum, we find for the reasons given that Petitioner has proved by a preponderance of the evidence that a person of ordinary skill would have been motivated to combine Tajima and Foster in the manner described.

At the oral argument, in discussing this ground Petitioner's counsel indicated that Petitioner was not arguing that this combination of references does not meet a claim limitation. Hearing Tr. 119:3–13. We, therefore, determine for the reasons given that Petitioner has demonstrated that claim 1

would have been obvious in light of Tajima and Foster. Claim 9 is essentially identical to claim 1. Neither claim 9 nor dependent claims 2 and 11–14 have been separately argued by Patent Owner. Accordingly, for the reasons given for claim 1, we determine that Petitioner demonstrates that those claims also would have been obvious over Tajima and Foster.

4. Tajima and Rivest

In the last two of the four Tajima grounds, Petitioner contends that claims 9–14 would have been obvious in light of Tajima and Rivest and claims 1–3 and 6 would have been obvious in light of Tajima, Rivest, and Shyu. Pet. 46–51; Bhattacharjee I Decl. ¶¶ 180–199. Rivest discloses "a new mode of encryption for block cyphers." Ex. 1034, 210. Rivest calls this "all-or-nothing" encryption. *Id.* Petitioner asserts that a person of ordinary skill "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 (citing Ex. 1034, 212–214; Bhattacharjee I Decl. ¶ 184–185).

Patent Owner responds that "Petitioner's proffered motivation should also be rejected because it is contradicted by Rivest itself." PO Resp. 29. Patent Owner asserts that "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.'" *Id.* (citing Ex. 1034, 212). More specifically, "AoNT adds additional protection to a data set that is otherwise separately encrypted or secured." *Id.*

We agree with Patent Owner that Petitioner fails to demonstrate a sufficient motivation to combine Tajima with Rivest as proposed in the Petition. Consistent with Patent Owner's argument, Rivest itself explains "[w]e note that the all-or-nothing transformation is not itself 'encryption,'

since it makes no use of any secret key information." Ex. 1034, 212. Rivest continues, "[i]t is merely an invertible 'pre-processing' step that has certain interesting properties." *Id.* We find further support in the testimony of Dr. Rubin that "a [person of ordinary skill] would not be motivated to apply Rivest's AoNT using the user's public key as Petitioner suggests." Rubin II Decl. ¶ 84. Dr. Rubin explains, "Rivest says nothing about the use of public keys and is not designed to be used with public keys." *Id.* Furthermore, he testifies that "[i]nstead of a public key, Rivest requires the use of a random number as the basis for its AoNT transformation." *Id.* (citing Ex. 1034, 213–214). We agree with this reasoning and find it persuasive.

We find that Petitioner does not persuasively respond to Patent Owner's arguments. Pet. Reply. 19–20. For example, Petitioner does not persuasively address Rivest's own disclosure that AoNT is "merely an invertible 'pre-processing' step," and not an encryption. Ex. 1034, 212. For the reasons given, we find that Petitioner has failed to demonstrate by a preponderance of the evidence a sufficient motivation to combine Tajima and Rivest.[7]

Shyu discloses "a method and system for dynamic data encryption, wherein the scrambling algorithm and the key word for the source data are dynamically changed to effectively guard against piracy when data is

[7] We are not persuaded otherwise by Petitioner's citation of an embodiment in the '116 patent using AoNT. Pet. 47 (citing Ex. 1001, 77:13–43). The Federal Circuit has cautioned that "[t]he inventor's own path itself never leads to a conclusion of obviousness; that is hindsight. What matters is the path that the person of ordinary skill in the art would have followed, as evidenced by the pertinent prior art." *Millennium Pharms., Inc. v. Sandoz Inc.,* 862 F.3d 1356, 1367 (Fed. Cir. 2017) (quoting *Otsuka Pharm. Co., Ltd. v. Sandoz, Inc.*, 678 F.3d 1280, 1296 (Fed. Cir. 2012)) (alteration in original).

transferred between two entities, such as a transmitter and a receiver of a data processing system." Ex. 1016, 1:35–41. Petitioner contends "it would have [been] obvious to vary the encryption algorithm in Tajima's system." Pet. 48. Petitioner asserts a person of ordinary skill "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." *Id.* (citation omitted). Patent Owner responds that "*no* [person of ordinary skill] would be motivated [to] 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." PO Resp. 32–33.

Dr. Rubin explains that Kerckhoff's Principle "holds that a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge." Rubin II Decl. ¶ 94. Citing this testimony, Patent Owner argues, "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." PO Resp. 33.

Petitioner does not persuasively respond to this argument. Pet. Reply 20–21. Petitioner argues that "Shyu does not use secret algorithms." *Id.* at 20. Instead, according to Petitioner "Shyu selects from among *known* algorithms to secure different data segments." *Id.* However, we find Shyu's disclosure that "the scrambling algorithm and the key word for the source data are dynamically changed to effectively guard against piracy" is telling evidence that the underlying algorithms themselves are not secure, and therefore Kerckhoff's principle applies here. *See* Ex. 1016, 1:37–39. We also find persuasive reasoning in Patent Owner's assertion that "[c]ombining

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." PO Resp. 34–35.

In sum, for the reasons given, we agree with Patent Owner that Petitioner fails to prove sufficiently that a person of ordinary skill would have been motivated to combine Tajima and Rivest. Further, Petitioner fails to demonstrate that even assuming that Tajima and Rivest would have been combined, a person of ordinary skill would have further combined their teachings with Shyu.

5. Summary and Conclusion – Tajima Grounds

For the foregoing reasons, Petitioner has demonstrated by a preponderance of the evidence that claims 1, 2, 9, and 11–14 would have been obvious over Tajima and Foster. Petitioner has failed to prove that claims 1 and 5–8 are anticipated by Tajima or would have been obvious over Tajima alone.

Furthermore, Petitioner has failed to demonstrate by a preponderance of the evidence that claims 9–14 would have been obvious over Tajima and Rivest, or that claims 1–3 and 6 would have been obvious over Tajima, Rivest, and Shyu.

D. Foster-Hayhurst Ground

1. Introduction

Petitioner's fifth ground asserts that claims 1, 2, 5, 9, and 11 would have been obvious over the combination of Foster and Hayhurst. *See supra*, Section I.H. As with the grounds based on Tajima, Petitioner provides an element-by-element analysis, supported by testimony from Dr. Bhattacharjee. Pet. 51–77; Bhattacharjee I Decl. ¶¶ 212–275.

Focusing on claim 1, Petitioner contends that Foster's encryption method generates a plurality of payloads by parceling digital content, which Petitioner identifies as the claimed "data set." Pet. 68 (citing Ex. 1006 ¶ 64). Petitioner explains that these content packets or payloads 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)." *Id.* at 69 (citing Bhattacharjee I Decl. ¶ 256). Petitioner asserts the corresponding limitations in claim 9 are identical and relies on the same analysis as for claim 1. *Id.* at 75 (citing Bhattacharjee I Decl. 269).

Petitioner contends a person of ordinary skill "would have had 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 (e.g., consumer set-top boxes) as Hayhurst teaches." Pet. 61–62 (citing Bhattacharjee I Decl. ¶ 240).

Patent Owner responds with three principal arguments. First, Patent Owner contends that Petitioner fails to prove that Hayhurst is analogous art to the '116 patent. PO Resp. 38–47. Second, Patent Owner contends Petitioner fails to demonstrate that a person of ordinary skill would have combined the teachings of Foster and Hayhurst as proposed by Petitioner. *Id.* at 47–68. Finally, Patent Owner contends that neither Foster nor Hayhurst discloses the claimed "data chunks." *Id.* at 68–69. We discuss these issues in the following sections.

2. Analogous Art

The Federal Circuit has described the test for analogous art in the following terms:

> The analogous-art test requires that the Board show that a reference is either in the field of the applicant's endeavor or is reasonably pertinent to the problem with which the inventor was concerned in order to rely on that reference as a basis for rejection.

In re Kahn, 441 F.3d 977, 986-87 (Fed. Cir. 2006) (citing *In re Oetiker*, 977 F.2d 1443, 1447 (Fed. Cir. 1992)).

Patent Owner contends that "Hayhurst and the '116 patent do not share the same field of endeavor." PO Resp. 39. Patent Owner asserts that "[a]s Petitioner and Dr. Bhattacharjee admit, the '116's field is securing data while Hayhurst's is decentralized electronic media delivery." *Id.*; *see* Ex. 1001, 2:39–41 ("[O]ne aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use."); Bhattacharjee I Decl. ¶ 31. Patent Owner continues, "[t]hat [Hayhurst] 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 [patent]." PO Resp. 43.

We do not agree with Patent Owner and find that Hayhurst is analogous art to the '116 patent. As Petitioner points out, Hayhurst describes its "Technical Field" as "electronic media delivery . . . including the secure handling and storage of such media." Pet. Reply 21 (emphasis omitted) (quoting Ex. 1007 ¶ 2). At oral argument, Patent Owner's counsel agreed that a media file is data:

> [THE BOARD]: . . . Counsel, . . . are you contending that the media that's referred to here, the media file, that that's not data?
>
> [COUNSEL]: I'm not suggesting that at all, Your Honor.
>
> . . . .

> [THE BOARD]: . . . My question is: why wouldn't a person of ordinary skill in the art consider a media file data?
>
> [COUNSEL]: I am not disputing that, Your Honor. I believe a person of ordinary skill in the art would consider a media file to be data.

Hearing Tr. 78:4–7, 78:15–19. Thus, we see little difference, if any, between Hayhurst's field of endeavor (including the secure handling of electronic media) and the field of the '116 patent ("securing data"). Consequently, we find that Petitioner has established that Hayhurst and the '116 patent share the same field of endeavor (securing handling of data), and therefore Patent Owner's non-analogous art argument is unavailing.

3. Motivation to Combine Foster and Hayhurst

Petitioner provides several persuasive reasons that would have motivated a person of ordinary skill to combine the teachings of Foster and Hayhurst with a reasonable expectation of success. Pet. 61–67; Bhattacharjee I Decl. ¶¶ 240–253. Among these are the goal of improving the delivery of content to consumer devices. *See* Pet. 62–63; Bhattacharjee I Decl. ¶¶ 240–241. Petitioner explains that where a content service provider implements Foster's encryption system, a person of ordinary skill would have been motivated to configure the content provider "to distributively store Foster's segmented content units on multiple devices as taught by Hayhurst." Pet. 62–63; Bhattacharjee I Decl. ¶¶ 242–244. This would achieve "Hayhurst's explicitly taught benefits . . . in improving delivery of digital content . . . and well-known benefits of distributive-storing techniques like Hayhurst's." Pet. 63. The improvements would include "improvements to: (1) speed of accessing content by a subscriber because segments would be retrieved from multiple sources, thus avoiding single-

source bottlenecks; and/or (2) efficiency by intelligently selecting storage device(s) that would provide the best delivery based on availability, location, etc." *Id.* (citing Bhattacharjee I Decl. ¶¶ 242–244). For the reasons given, we find that a person of ordinary skill would have recognized significant benefits in combining the teachings of Foster and Hayhurst.

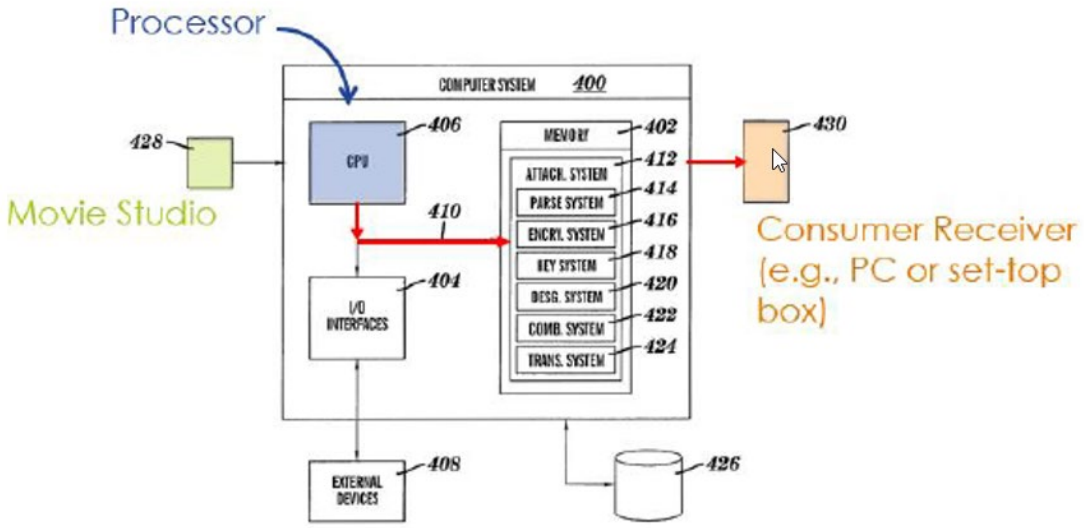
Patent Owner responds that a person of ordinary skill "would not be motivated to combine Foster and Hayhurst because they are incompatible and have conflicting goals." PO Resp. 47. Patent Owner argues that "Foster is directed towards real-time streaming of television and live events." *Id.* at 47–48. Thus, Foster "is concerned with avoiding delays that interfere with immediate access to content (*e.g.*, when a user changes a channel)." *Id.* at 48. Patent Owner argues that in contrast, Hayhurst "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." *Id.*

Petitioner responds to Patent Owner's incompatibility argument by pointing out that Foster's teachings are not limited to live-streaming. Pet. Reply 24–26; Bhattacharjee II Decl. ¶¶ 109–127. In addition, Foster teaches storing encrypted content, such as video-on-demand. *Id.* at 24 (citing Ex. 1006 ¶ 64; Bhattacharjee II Decl. ¶¶ 102–111). We agree with Petitioner and find for the reasons given that Foster is not limited to live-streaming and also discloses storing encrypted video data for video-on-demand applications. Thus, we do not agree with Patent Owner's arguments based on alleged "incompatibility" between Foster and Hayhurst. *See* PO Resp. 47; PO Sur-reply 17–20. We discuss this also in Section II.C.3, *supra*. Our further reasoning follows.

This dispute between Petitioner and Patent Owner over the disclosure of storing video information in Foster began with the Petition and

Preliminary Response. Pet. 51–54; Prelim. Resp. 25–27; *see also* Section II.B, *supra* (Claim Construction). The description of Foster in the Petition includes the following disclosure of storing encrypted keys and content: "Finally, encrypted key 112, encrypted content packet 114, and header 104 are combined as a processed content unit 116, which *can be stored* by a recipient in a receiver (e.g., stored in a consumer's set-top box)." Pet. 52 (citing Ex. 1006 ¶¶ 64, 40, 41; Bhattacharjee I Decl. ¶¶ 217–220) (internal quotation marks omitted, emphasis added). Patent Owner responded by urging an implicit construction of "storage device" that would have required "secure long-term storage." *See* Institution Dec. 12–13; Prelim. Resp. 34–37 Based on that construction, Patent Owner argued that "a [person of ordinary skill] 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 [patent]—'magnetic or optical disk, USB key drive, etc.'—are each devices primarily dedicated to long-term storage." Prelim. Resp. 37.

In our Institution Decision, we said we were "skeptical" of this construction proposed by Patent Owner. Institution Dec. 12. However, we determined that "we need not resolve whether the claims require long-term storage at this stage because we disagree with Patent Owner that this feature distinguishes the systems resulting from combining Foster with Tajima or Hayhurst." *Id.* at 13. Specifically with respect to Foster, we found that "Foster alone provides a sufficient teaching of storage." *Id.* at 21. In support of our finding, we cited Foster's Figure 16, as annotated by Dr. Rubin, following.



Rubin Decl. ¶ 72. Foster's Figure 16 (annotated) shows video content being sent from movie studio 428 to computer system 400 to receiver 430. *Id.* We explained in our Institution Decision that Dr. Rubin identifies receiver 430 as "a PC or set-top box." Institution Dec. 21 (citing Rubin Decl. ¶ 72). We also explained that Foster describes how this receiver stores encrypted video content. *Id.* at 21–22 (citing Ex. 1006 ¶¶ 8, 79). According to Foster, "[t]he encrypted title key is then attached to the content packet and the header for synchronized transmission to, or storage by a receiver." *Id.* at 21 (quoting Ex. 1006 ¶ 8). For the reasons given, we find that Foster specifically describes storing movies in a PC or a set-top box, as in Dr. Rubin's example. *See* Ex. 1006 ¶¶ 6, 79.[8]

Central to Patent Owner's argument for Foster's "incompatibility" is Patent Owner's misapprehension that Foster is limited to streaming. PO

[8] Dr. Rubin does not dispute that Foster discloses storage; he testifies, instead, that Foster's system does not "even store each chunk on a plurality of different storage devices, as required by the '116's independent claims." Rubin I Decl. ¶ 73. Dr. Rubin's testimony is not persuasive because it fails to address the distributed storage in the combination of Foster and Hayhurst.

Resp. 47–68. For example, Patent Owner's arguments that Foster's goal is "avoiding delays" or "synchronizing the transmission of encrypted content packets with the keys" are predicated on Patent Owner's contention that "Foster is directed towards real-time streaming of television and live events." *Id.* at 47–56. As discussed *supra*, we find that Foster is not limited to streaming, but also discloses storage of video data for video-on-demand applications. As further evidence of this feature of Foster, Petitioner cites Foster's references to DRMs (Digital Rights Management Systems), as well as CAS (Conditional Access Systems) and MPEG-standard program streams, that are indicative of video-on-demand capabilities. Pet. Reply 24–26. For example, Petitioner points to Foster's Figure 1, below, as evidence of storing encrypted video content in Foster. Pet. Reply 25–26.

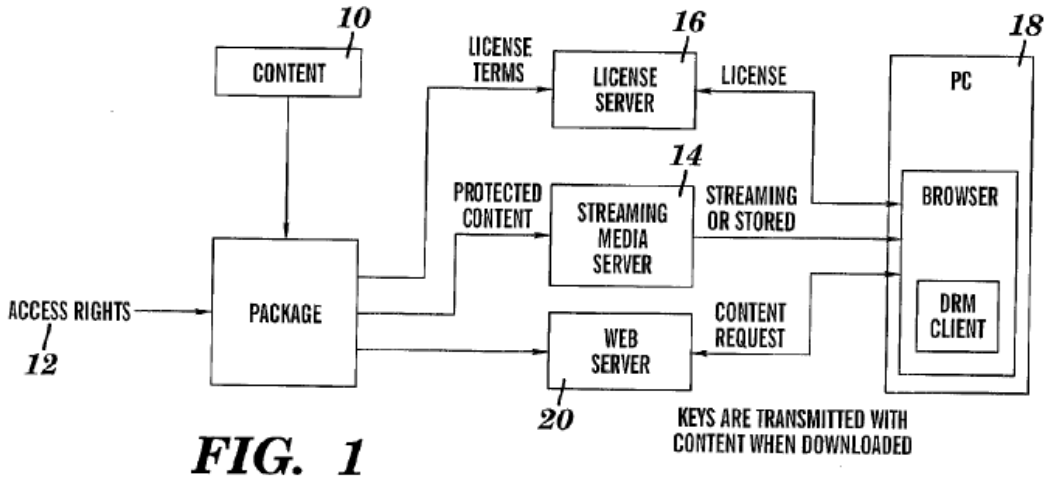


FIG. 1

Figure 1 is a flow diagram for a DRM system that streams or stores content. *See id.* (citing Ex. 1006 ¶¶ 5, 49; Bhattacharjee II Decl. ¶¶ 118–120).

As shown in Figure 1, the link between streaming media server 14 and PC 18 is labeled "STREAMING OR STORED." Dr. Bhattacharjee testifies that "in Foster's DRMS implementations, content is packaged and loaded [i.e., stored] onto a web server and subsequently downloaded to [i.e., stored

at a] personal computer for on-demand accessing at rendering time (i.e., when the user wants to view stored content at some indefinite time after downloading/storing)." Bhattacharjee II Decl. ¶ 118 (citing Ex. 1006, ¶¶ 5, 49) (alterations in original) (internal quotation marks omitted). This description further confirms our finding that Foster is not limited to streaming and discloses storing video data for on-demand access.

We further disagree with Patent Owner that combining Foster's teachings with Hayhurst would "thwart Foster's goals, make Foster inoperable for its intended purpose, and compromise any security benefits otherwise provided by Foster alone." PO Resp. 57–68. To the extent that Patent Owner's arguments are based on its contention that Foster is limited to streaming, those arguments are addressed above. *See supra*; *see also* Pet. Reply 25–27. As to the benefits of combining Foster and Hayhurst, Petitioner cites the higher level of security that would result from using Hayhurst's distributed storage with Foster. *Id.* at 28. We find this argument persuasive that the benefits of combining Foster and Hayhurst would have outweighed any drawbacks alleged by Patent Owner, most of which are predicated on an overly narrow and erroneous reading of Foster as limited to streaming. *See* Pet. Reply 27–29:

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

Other benefits of combining Foster and Hayhurst are cited in the Petition. *See* Pet. 62–63. These include improving content delivery "in multiple

ways" such as improved speed and efficiency. *Id.* (citing Bhattacharjee I Decl. ¶¶ 241–244).

Lastly, we address Patent Owner's argument that Petitioner has "improperly change[d] its unpatentability theory." PO Sur-reply 20–23. Patent Owner complains that "[s]pecifically, Petitioner argues that 'Foster's teachings are not limited to livestreaming' as 'Foster teaches storing encrypting content for and by recipient(s) (*e.g.*, video-on-demand).'" *Id.* at 21 (citing Pet. Reply 21). As is demonstrated above, however, the dispute between Petitioner and Patent Owner over the disclosure of storing video information in Foster began with the Petition and Preliminary Response. Patent Owner's suggestion of surprise and prejudice is without merit.

Nor are we persuaded by Patent Owner's response to Petitioner's arguments based on Foster's disclosure of video-on-demand systems. PO Sur-reply 20–26. For example, Patent Owner argues that "Foster's inventive system is intended to replace both DRMS and CAS." *Id.* at 24. In another example, Patent Owner asserts that "[w]hether DRMS allegedly stores an entire content file on a personal computer has no bearing on whether Foster's system does." *Id.* at 25. Still further, regarding MPEG, Patent Owner argues "[t]hat a content file may be stored in 'fixed storage' does not suggest that Foster teaches that the entire content file is stored on a personal computer in its system." *Id.* We do not find these arguments convincing. The references to DRMs, CAS, and MPEG advanced by Petitioner are not intended as "description[s] of prior art," as Patent Owner asserts. *Id.* at 20. Petitioner presents these as exemplary applications of Foster's teachings of storing video data. For example, Petitioner asserts that "Foster is explicit that synchronization reduces latency for storage-based purposes, like for Digital Rights Management Systems ('DRMSs')." Pet. Reply 25. Similarly,

"[c]onsistent with its DRMS disclosures, Foster teaches processing datasets for the MPEG-standard's 'program stream,' which Foster says is intended for use 'in fixed storage.'" *Id.* at 26 (emphasis omitted). "Finally, Foster's streaming in a conditional access system ('CAS') is not limited to streaming 'live' broadcasts." *Id.*

In sum, after considering Petitioner's evidence and Patent Owner's opposition, for the reasons given we find that Petitioner has demonstrated a motivation to combine the teachings of Foster and Hayhurst.

4. "Plurality of Data Chunks" Limitation

Claim 1 recites "distributing the data set into a plurality of data chunks, wherein none of the data chunks are, by themselves, sufficient to reconstruct the data set" and "encrypting each of the data chunks with a respective one of a plurality of encryption keys." *See* Claim Limitations IA, 1B in Section I.E, *supra*. Claim 9 recites the same limitations. Ex. 1001, 100:63–67.

Petitioner contends that Foster's encrypted payloads are the claimed "data chunks." *See* Pet. 68–69. Patent Owner disagrees, arguing that "Foster . . . operates on MPEG video packet payloads and does not disclose generation of data chunks." PO Resp. 18 (emphasis omitted). Patent Owner asserts, "[t]here is no reason to assume that a [person of ordinary skill] would understand that Foster's packet payload corresponds to the data chunk of the '116 or the data fragment of Tajima." *Id.* at 20. Patent Owner continues, "Foster's packet payloads are merely a by-product of the MPEG streaming standard." *Id.* at 21.

We disagree with Patent Owner that Foster's payloads are not "chunks." As Petitioner points out in its Reply, each Foster payload is a portion of Foster's content, and thus none by themselves are sufficient to

reconstruct Foster's content. Pet. Reply 29. Dr. Bhattacharjee testifies that "Foster's payloads meet the claimed *data chunks* and Foster's content meets the *claimed data set*." Bhattacharjee II Decl. ¶ 183. He continues, "Foster's payloads are each only a portion of Foster's content and thus *none* of [Foster's payloads] are, by themselves, sufficient to reconstruct [Foster's content]." *Id.* (alteration original; internal quotation marks omitted). He concludes, "[t]hat is all claims 1 and 9 require of the claimed *data chunks*." *Id.*

We agree with Petitioner's argument and with Dr. Bhattacharjee's testimony because they are supported by the '116 patent and the plain meaning of "data chunks." Citing the '116 patent specification for support, Dr. Bhattacharjee testifies, "[i]n my opinion, a [person of ordinary skill] understood from the '116 specification that a data chunk is simply a portion (or part) of the data set—i.e., a subset of the data set—and that nothing in the '116 patent supports a narrow interpretation of data chunk that excludes Foster's payloads." Bhattacharjee II Decl. ¶ 187 (emphasis omitted) (citing Ex. 1001, 21:44–22:4; 58:58–62; 75:15–19; 77:51–82:2).

On the other hand, Patent Owner advances a special meaning for data chunks that excludes data packets. PO Resp. 68–69. But Patent Owner has not proposed a special construction for this claim term. In the absence of any claim construction proposals from Patent Owner, we adopted plain meaning as the claim construction standard for this Decision. *See* Section II.B, *supra*. For the reasons given, we find that the plain meaning of data chunks is that spelled out in the language of the claims, namely, parts of the data set that are not, "by themselves, sufficient to reconstruct the data set." Ex. 1001, 100:22–23; 100:63–64. As such, we find that Foster's payloads are data chunks because Foster's payloads are portions of Foster's content,

and by design they are not sufficient by themselves to reconstruct Foster's content. Pet. 68–69; Bhattacharjee I Decl. ¶ 256; *see also* the description of Foster in Section I.E.2, *supra*.

5. Summary and Conclusion – Foster-Hayhurst Ground

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that independent claims 1 and 9 would have been obvious over Foster and Hayhurst. Patent Owner does not separately argue dependent claims 2, 5, and 11 challenged in this ground. Therefore, for the reasons given for claims 1 and 9, we determine that Petitioner has demonstrated also that those claims would have been obvious over Foster and Hayhurst. *See* Pet. 74–77; Bhattacharjee I Decl. ¶¶ 267–268, 275.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has proved by a preponderance of the evidence that claims 1, 2, 5, 9, and 11–14 of the '116 patent are unpatentable. Petitioner has not proved by a preponderance of the evidence that claims 3, 6–8, and 10 of the '116 patent are unpatentable. In summary:

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 5–8	102	Tajima		1, 5–8
1, 5–8	103	Tajima		1, 5–8
1, 2, 9, 11–14	103	Tajima, Foster	1, 2, 9, 11–14	
9–14	103	Tajima, Rivest		9–14

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1–3, 6	103	Tajima, Rivest, Shyu		1–3. 6
1, 2, 5, 9, 11	103	Foster, Hayhurst	1, 2, 5, 9, 11	
Overall Outcome			1, 2, 5, 9, 11–14	3, 6–8, 10

IV. ORDER

For the foregoing reasons, it is, therefore:

ORDERED that Petitioner has demonstrated by a preponderance of the evidence that claims 1, 2, 5, 9, and 11–14 of the ’116 patent are unpatentable;

FURTHER ORDERED that Petitioner has not demonstrated by a preponderance of the evidence that claims 3, 6–8, and 10 of the ’116 patent are unpatentable;

FURTHER ORDERED that because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.[9]

[9] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

FOR PETITIONER:

Elisabeth H. Hunt
Richard F. Giunta
Marc S. Johannes
Gregory S. Nieberg
WOLF, GREENFIELD & SACKS, P.C.
ehunt-ptab@wolfgreenfield.com
rgiunta-ptab@wolfgreenfield.com
mjohannes-ptab@wolfgreenfield.com
gnieberg-ptab@wolfgreenfield.com

FOR PATENT OWNER:

Stephen J. Elliott
Andrei Iancu
Haley M. Sanders
SULLIVAN & CROMWELL LLP
elliotts@sullcrom.com
iancua@sullcrom.com
sandersh@sullcrom.com

Kenneth Weatherwax
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com