

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, STEPHEN E. BELISLE, and
DANIEL KHAZDAN, *Administrative Patent Judges*.

GIANNETTI, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

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.”).

To institute an *inter partes* review, we must determine “that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a) (2018). For the reasons discussed below, Petitioner has shown a reasonable likelihood that it would prevail with respect to at least one claim challenged in the Petition. Thus, we institute an *inter partes* review.

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 indicates that IPR2024-00213, IPR2024-00214, and IPR2024-00215 are related matters. Paper 4, 1; Paper 9, 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 cryptographic parsing and splitting of the encrypted file into two or more portions or shares, 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, 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 57:10–24.

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

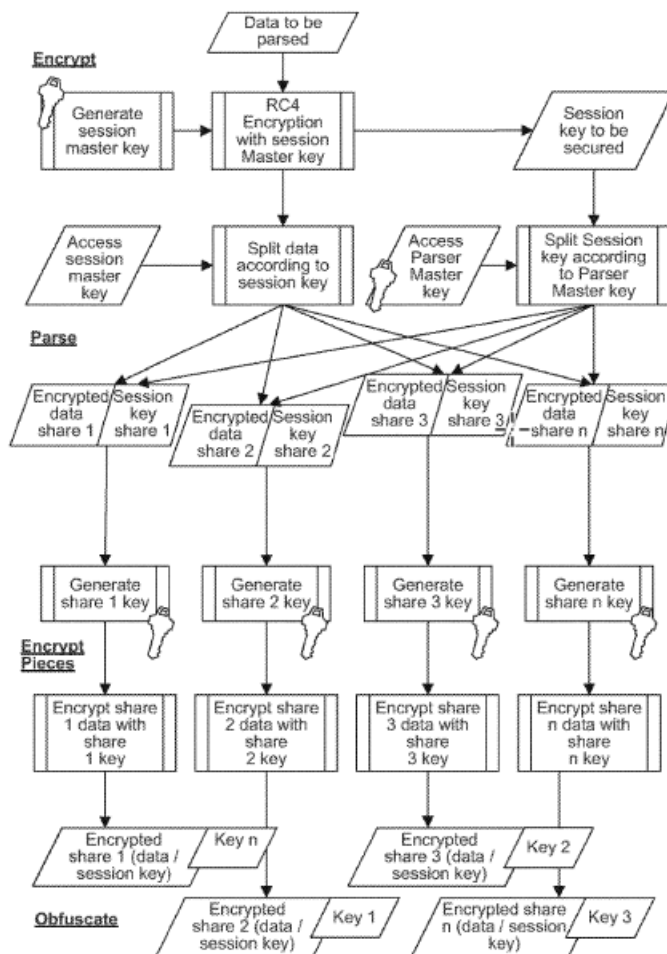


FIG. 21

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.

Ex. 1001, 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

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, <i>All-or-Nothing Encryption and the Package Transform</i> , Fast Software Encryption, 4 th Intl. Workshop, FSE’97, Jan. 20–22, 1997 Proceedings, pp. 210–218.	1034

In addition, Petitioner relies on the Declaration of Samrat Bhattacharjee, Ph.D. Ex. 1003 (“Bhattacharjee Decl.”). Patent Owner submits the Declaration of Aviel D. Rubin, Ph.D. Ex. 2003 (“Rubin Decl.”).

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

G. Asserted Grounds

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

Claims Challenged	Pre-AIA² 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

H. Overview of the Principal Prior Art Asserted

1. Tajima

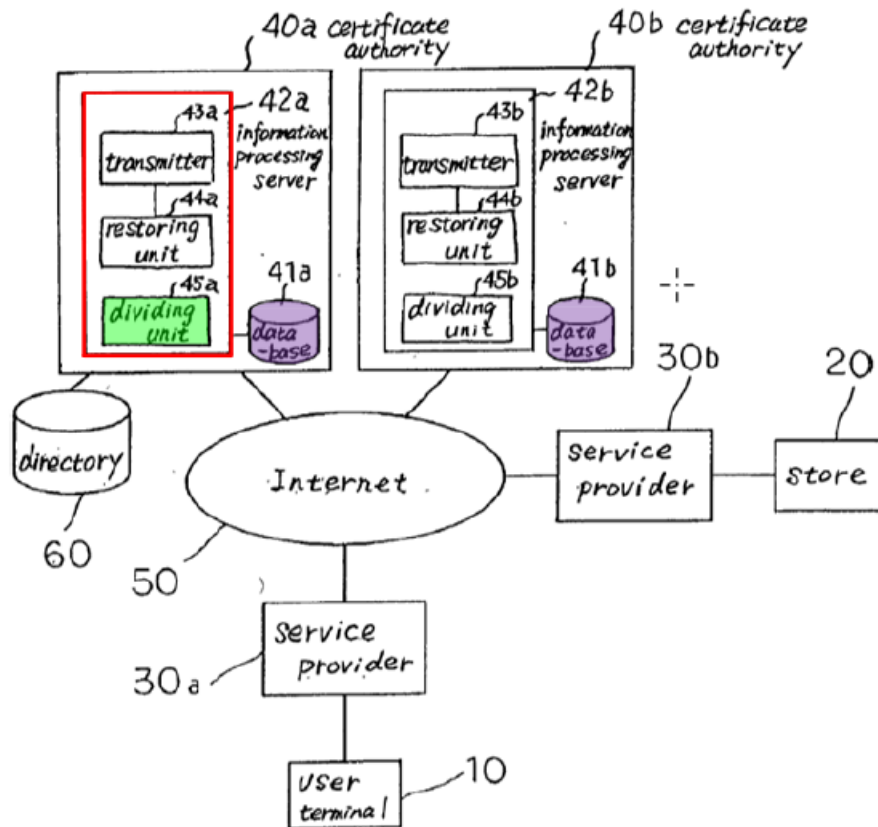
Tajima discloses “a personal information management system and a personal information management method for managing personal information by means of areas that are connectible to the Internet.”

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 Abstr. 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.*

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

² 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”), and we therefore apply the pre-AIA versions of 35 U.S.C. §§ 102 and 103.

Fig. 5



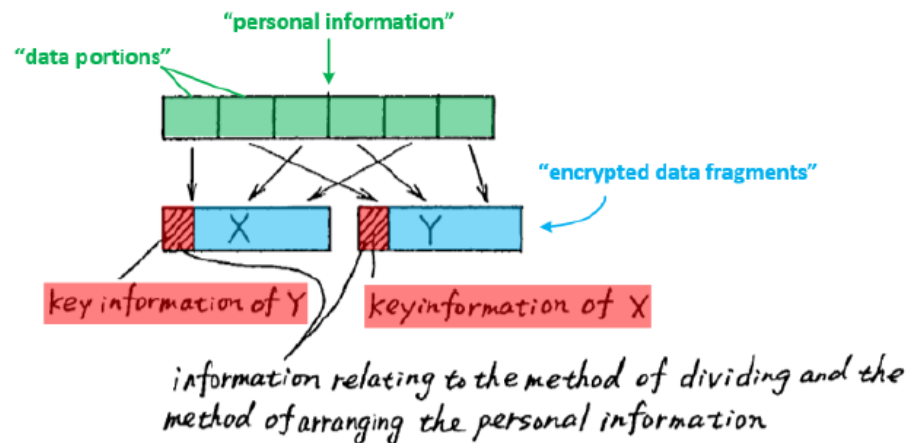
As shown in annotated Figure 5, this embodiment is made up of user terminal 10 that is connectible to Internet 50; service provider 30a to which user terminal 10 subscribes for handling connections of user terminal 10 to Internet 50; certificate authority 40a for both certifying personal information 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.

Fig. 12



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.

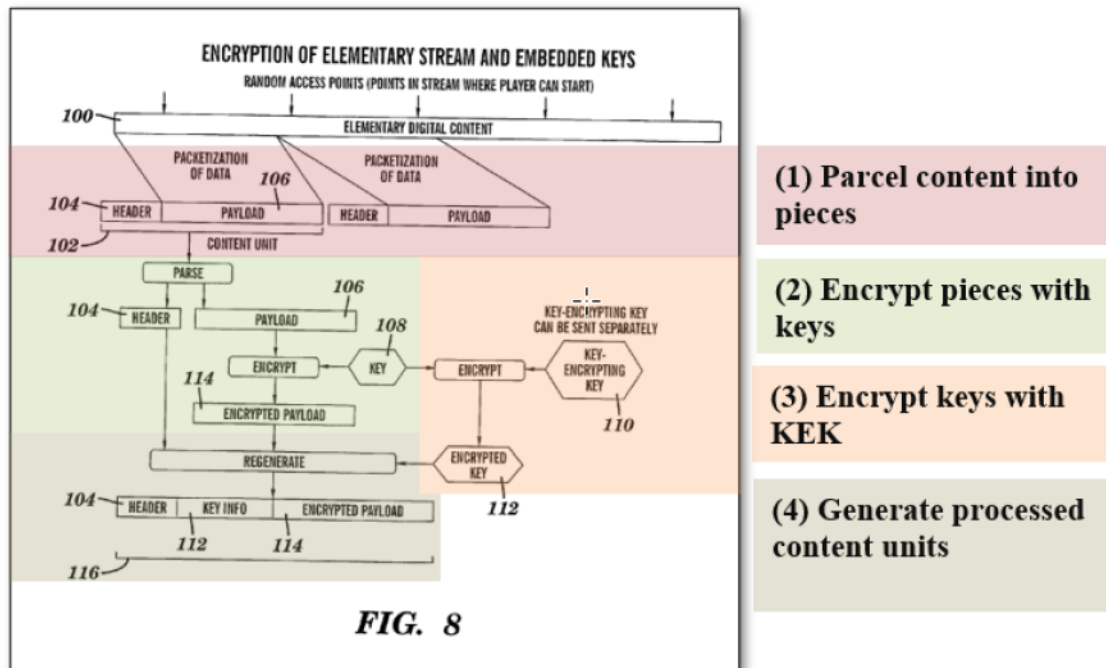


Figure 8 is annotated by Petitioner with labels on four different parts of Foster's method: (1) parceling digital content 100 into content units 102 containing header 104 and payload 106, (2) encrypting payload 106 with title key 108 to yield content package 114, (3) encrypting each key 108 with key-encrypting 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.

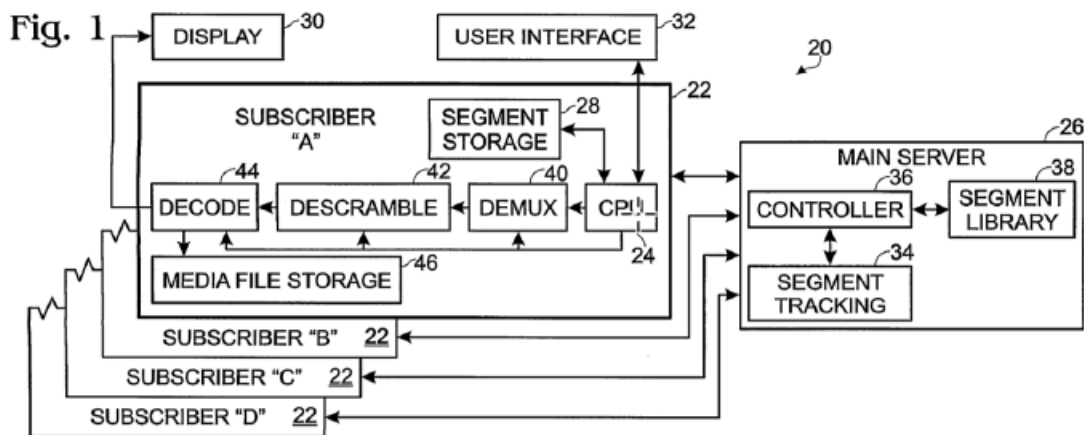


Figure 1 is a block diagram of Hayhurst's system for decentralized media delivery. Ex. 1007 ¶ 12. Each subscriber unit 22 includes storage device 28, such as a conventional hard disk. *Id.* ¶ 18. This storage device stores segments of one or more media files (e.g., movies). *Id.* In Figure 1, each unit 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 also asserts that a “higher level of education may substitute for less experience.” *Id.*

At this stage, Patent Owner does not oppose Petitioner’s assertions or provide a definition of a person of ordinary skill in the art. *See* Prelim. Resp.; Rubin Decl. ¶ 20 (accepting Dr. Battacharjee’s proposed qualifications for the purposes of his declaration). We regard 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 decision, we adopt Petitioner’s proposal.

B. *Claim Construction*

“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)).

Neither party explicitly proposes constructions for disputed claim terms. Petitioner acknowledges the existence of “competing proposed constructions” in the parallel district court action. Pet. 7 (citing Ex. 1042, 1043). Petitioner contends 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.*

For its part, Patent Owner does 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). *See infra*, Sections II.C & D.

Notwithstanding the absence of any explicit claim construction proposals from the parties, and after reviewing the parties’ submissions, the Board provides the following guidance, based on the record at this stage in the proceeding.

I. “storage devices”

Claim 1 recites “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.” Limitation 1D; Ex. 1001, 100:28–31. Claim 9 recites a similar limitation (substituting “transformed” for “obfuscated.”). *Id.* at 101:3–6.

Patent Owner argues that the recited “storage device” requires “secure long-term storage.” Prelim. Resp. 34. Patent Owner contends 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.” *Id.* at 37.

We note that the claims do not use the term “long-term” in referring to storage devices. *See Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) (“First, we look to the words of the claims themselves, . . . to define the scope of the patented invention.”). Nor do we see support in the ’116 specification for limiting the claims to “long-term storage,” which, itself, would require further construction to determine what qualifies as “long-term.” We are, therefore, skeptical of Patent Owner’s proposed limitation of the term “storage device.”

However, 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. *See* discussion in Sections II.C.2 and II.D, *infra*.

2. *Other Constructions*

At present, we do not see the need for further constructions to resolve this controversy. *See Vivid Techs.*, 200 F.3d at 803.

C. *Tajima Grounds*

1. *Introduction*

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

In its Preliminary Response, Patent Owner does not address separately these four grounds based on Tajima. Instead, Patent Owner addresses two limitations that are common to all Tajima grounds, without distinguishing among the four grounds that are separately set forth in the Petition. Moreover, Patent Owner focuses its analysis on Tajima, and not the other

references combined with Tajima in Petitioner’s second, third, and fourth grounds.

In our analysis below, for the purpose of institution, we focus on one of the four Tajima grounds as exemplary. *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.”). Although not required for institution under *SAS Inst.*, we also provide guidance on the Foster-Hayhurst ground. *See infra*, Section II.D,

2. *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. 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 Decl. ¶¶ 164–167. Petitioner provides a similar analysis for claim 9 and the dependent claims. Pet. 42–46; Bhattacharjee Decl. ¶¶ 170–175. Petitioner asserts that a person of ordinary skill would have combined the teachings of those references with a reasonable expectation of success. Pet. 37–40; Bhattacharjee Decl. ¶¶ 155–163.

As noted above, Patent Owner’s response is the same for each of the challenges based on Tajima. *See* Prelim. Resp. 3–24. Also, Patent Owner does not separately address the dependent claims. Instead, Patent Owner focuses its response on two limitations appearing in both independent claims 1 and 9. Patent Owner contends Petitioner fails to demonstrate that Tajima meets these limitations. *Id.* at 3.

a. “*Separately Storing*” Limitation

Claim 1 (and claim 9) call for “*separately storing* each data chunk of the plurality of data chunks.” *See* limitation 1D *supra* (emphasis added); Ex. 1001, 101:3–4. Petitioner contends that this limitation is met by Tajima alone and by the Tajima-Foster combination. Pet. 40–41 (citing Bhattacharjee Decl. ¶ 164).

Patent Owner contends that “Tajima never says that its data fragments are ‘*stored*’ in databases 41a and 41b.” Prelim. Resp. 4. Patent Owner continues, “[r]ather, Tajima indisputably, consistently, and repeatedly tells us the data fragments are ‘*registered*.’” *Id.*

We agree that Tajima uses the term “register” in relation to the data fragments and the data base. *See, e.g.*, Ex. 1005 ¶ 67. However, Tajima also uses the term “register” elsewhere where it is clear that data is being stored. For example, in describing Figure 1, a “typical online shopping system,” Tajima discloses “a terminal that is configured to allow connection to Internet 550, and database 521, in which is registered personal information relating to the user of user terminal 510, are provided at store 520.” *Id.* ¶ 8. Similarly, in discussing the Background of the Invention, Tajima describes storing a user’s “registered personal information” “within one area as a contiguous data file”:

[I]f the above-described personal information relating to a user *is registered with one area* that is connectible to the Internet, there is the danger that, because the information *registered with one area as a contiguous data file*, this information may be viewed by unauthorized access from the outside through a Security hole or by unauthorized access by someone inside the system, even though the information is *registered with an area* that is closed to the outside by means of the access control function of a server or a firewall.

Id. ¶ 42 (emphases added). We take from these and other examples that Tajima consistently uses “register” to indicate storage. We, therefore, do not agree with Patent Owner that because Tajima uses the term “registering,” it does not teach or suggest “separately storing.” Prelim. Resp 11 (“Tajima discloses ‘registering’ not ‘storing’”). This determination is supported by testimony from Dr. Bhattacharjee. As Dr. Bhattacharjee testifies, “[a person of ordinary skill] understood that when a data fragment is ‘registered’ with a data base the data fragment is stored on the corresponding storage media.” Bhattacharjee Decl. ¶ 71. He explains further that “[r]egistering may also include additional processes that databases conventionally use to record information about the stored data, . . . but the principal act of registering data with a database is storing the data so that it can be accessed as authorized.” *Id.*

Invoking the doctrine of inherency, Patent Owner asserts that “Petitioner must prove that when Tajima ‘registers’ a data fragment, it necessarily stores the fragment in or ‘on’ the database.” Prelim. Resp. 5. We disagree. Our conclusion that at this stage Petitioner demonstrates sufficiently that Tajima discloses storing does not rely on inherency. Instead, we rely on the use of “registering” by Tajima to indicate storage and the testimony of Dr. Bhattacharjee cited above on how a person of ordinary skill would understand that term.

We find unpersuasive Dr. Rubin’s testimony that Petitioner and Dr. Bhattacharjee have not “demonstrated that Tajima’s ‘registering’ teaches this limitation.” Rubin Decl. ¶ 38. Because we conclude on the record before us that Tajima itself indicates that “registration” with a data base implies storage, at this stage we agree with Dr. Bhattacharjee and disagree with Dr. Rubin.

In any event, this exemplary ground we are considering is based on the combination of Tajima and Foster, and not Tajima alone. As discussed *supra*, in Section I.H.1, Foster discloses encrypting plaintext keys with a key encrypting key (KEK). Foster also teaches transmitting and storing the encrypted keys with the encrypted data. Ex. 1006 ¶¶ 8, 64–71; *see also* discussion of storage in Foster in Sections II.D.2 & 4, *infra*.

Petitioner provides a motivation to combine the teachings of Tajima and Foster with a reasonable expectation of success. *See* Pet. 36–40. Petitioner contends that “[persons of ordinary skill] would have recognized that Tajima-Foster would have beneficially provided even further security . . . because encrypted data fragments/key pairs and the KEK needed to decrypt the keys are each stored on different databases under separate control of respective service sites.” Pet. 39. Furthermore, Dr. Bhattacharjee testifies that “to safely include encryption keys with encrypted data, Foster teaches encrypting the encryption keys.” Bhattacharjee Decl. ¶ 153.

In summary, we find at this stage for the reasons given that Petitioner demonstrates sufficiently that Tajima, both alone and combined with Foster, teaches or suggests the “separately storing” limitation.

b. “Together With” Limitation

Claim 1 calls for “separately storing each data chunk . . . *together with one of the plurality of obfuscated different encryption keys* on a plurality of different storage devices.” Limitation 1D, *supra* (emphasis added). Claim 9 has a similar limitation, in which “transformed” is substituted for “obfuscated.” Ex. 1001, 101:4–6. Petitioner contends this limitation is met by the key encryption techniques in the Tajima-Foster combination. Pet. 40–42; Bhattacharjee Decl. ¶¶ 164–167.

Patent Owner contends that “[i]n 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.” Prelim. Resp. 12. Patent Owner continues, “[a]s 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.’” *Id.* (second and third alterations in original). Patent Owner cites Tajima’s Figures 12 (reproduced *supra*) and 13, and to references in Tajima to “information regarding the key” and “key information.” *Id.* at 12–13 (citing Ex. 1005 ¶¶ 112–114). Patent Owner contends that a person of ordinary skill would not have understood from Tajima that a key itself is stored with the data fragments. *Id.* at 13–14.

Patent Owner’s argument is unavailing at this stage. Patent Owner does not address the Tajima-Foster combination. Foster discloses storing the encrypted key itself with the data. *See* Ex. 1006 ¶ 64. Petitioner asserts that Tajima’s teachings would have been combined with “Foster’s key-encryption technique.” *Id.* at 36–37. Petitioner explains that Foster’s technique includes “encrypting each key 108 with a key-encrypting key (KEK) 110 so *that encrypted key 112 . . . can be securely stored/transmitted with the encrypted payload.*” Pet. 37 (citing Ex. 1006 ¶¶ 64–71) (emphases added). Referring to Figure 8, *supra*, Foster discloses that “key encrypting key 110 is used to encrypt title key 108, which is then attached to content packet 106 along with header 104.” Ex. 1006 ¶ 64. The resulting processed content unit 116 can then be transmitted to a recipient for storage. *Id.*

In view of these disclosures, we are not persuaded by Patent Owner’s “inherency” and other arguments, or with Dr. Rubin’s testimony on this

limitation. Pet. 14–24; Rubin Decl. ¶¶ 49–69. Neither Patent Owner nor Dr. Rubin addresses the combination of Tajima with Foster.

We agree also that Petitioner presents a sufficient motivation to combine the teachings of Tajima and Foster. *See* discussion *infra*. At this stage, Patent Owner does not address this evidence. Instead, Patent Owner provides generalizations about Petitioner’s arguments and Tajima that do not address the teachings of Foster or the rationale for combining Foster with Tajima. *See* Prelim. Resp. 18–24. For the reasons given, we find that the combination of Tajima’s teachings of transmitting “key information” and Foster’s key-encryption technique, which involves transmitting and storing the encrypted key itself, is sufficient to meet this limitation at this stage.

3. *Summary and Conclusion – Tajima Grounds*

We have considered Petitioner’s analysis of the Tajima grounds and Patent Owner’s response. We determine that for the reasons given, Petitioner has demonstrated that there is a reasonable likelihood of prevailing on at least the Tajima-Foster challenge to independent claims 1 and 9. Patent Owner does not separately argue dependent claims 2 and 11–14 challenged in this ground. Therefore, for the reasons given for claims 1 and 9 and in the Petition, we determine also that Petitioner has also demonstrated that there is a reasonable likelihood of prevailing on the Tajima-Foster challenge to those claims. *See* Petitioner’s analysis of claims 2 and 11–14 at pages 42–46 of the Petition.

At this stage, for the purpose of institution, we do not see the need to address the other Tajima grounds that were not separately addressed by Patent Owner.

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.G. As noted *supra*, we provide guidance on the Foster-Hayhurst ground although not required for institution under *SAS Inst.* As with the grounds based on Tajima, Petitioner provides an element-by-element analysis, supported by testimony from Dr. Bhattacharjee. Pet. 67–77; Bhattacharjee Decl. ¶¶ 254–275.

In its Preliminary Response, Patent Owner does not address separately each claim challenged in this ground. Instead, Patent Owner addresses certain limitations that are common to claims 1 and 9. Prelim Resp. 27–37. We address these in the sections that follow.

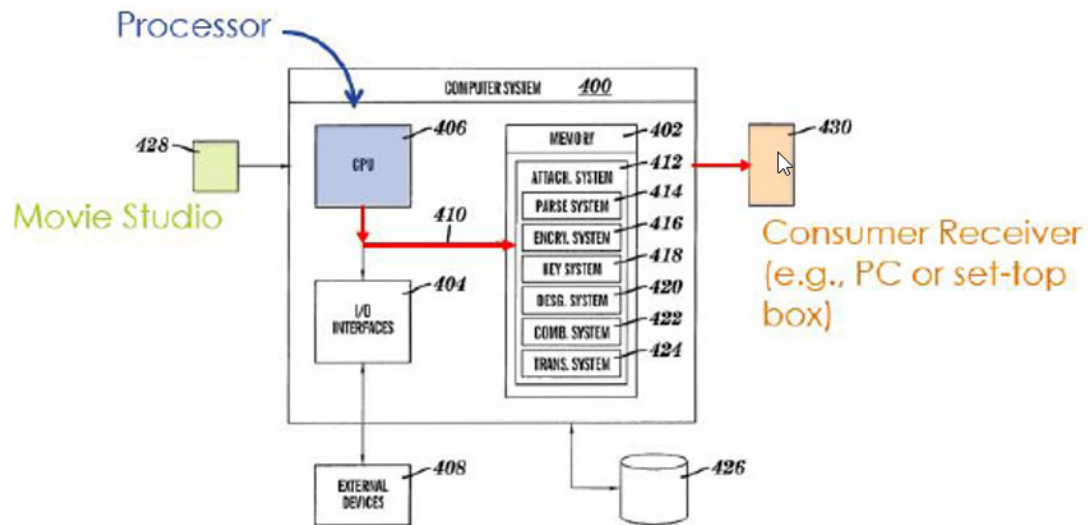
2. “Data Set” Storage Limitation

The preambles of claims 1 and 9 recite “a method for securing a data set.”³ Limitation 1[PRE], *supra*; *see also* claim 9 (Ex. 1001, 109:61–62). Petitioner asserts that the Foster-Hayhurst combination performs this “by encrypting digital content (i.e., a *data set* such as video data) using Foster’s encryption technique that provides enhanced security by using multiple encryption keys and provides a high level of security and a deterrence to piracy by applying Hayhurst’s distributed storage technique to Foster’s encrypted content.” Pet. 67–68 (citations and internal quotation marks omitted).

³ We do not express an opinion as to whether the preambles of the challenged claims are limiting.

Patent Owner contends “[t]he parties have now agreed that a ‘data set’ is ‘a collection of information *for storage*.’” Prelim. Resp. 27 (citing Petitioner’s district court claim construction brief, Ex. 2020). Patent Owner contends this preamble is limiting, that “Petitioner maps the ‘data set’ solely to Foster’s ‘content,’” and “Foster’s definition of ‘content’ makes no mention of ‘storage.’” *Id.* at 28. Patent Owner contends that Foster’s content is for streaming, not storage. *Id.* at 28. At this stage, we disagree with these arguments for the following reasons.

First, on this record, we find that Foster alone provides a sufficient teaching of storage. Foster’s Figure 16, with annotations by Dr. Rubin, is reproduced below.



Rubin Decl. ¶ 72. Figure 16 (annotated) shows content being sent from movie studio 428 to computer system 400 to receiver 430. Dr. Rubin identifies receiver 430 as “a PC or set-top box.” *Id.* Foster describes how this receiver stores encrypted content. *See* 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.*

¶ 8 (emphasis added). Foster further explains, “Once received, recipient 430 can then synchronously store the encrypted content.” *Id.* ¶ 79. For at least these reasons we determine that Foster sufficiently teaches that a PC or set-top box stores a version of the data set. Thus, we determine that Petitioner has sufficiently shown at this stage that Foster’s data set is “for storage.” *See* Pet. 51–53; Bhattacharjee Decl. ¶¶ 214–215, 220.

At this stage, we find unpersuasive Dr. Rubin’s testimony that Foster’s receiver is not a “storage device” because it does not provide “long-term storage” or is unlike the ’116 patent’s storage devices. *See* Rubin Decl. ¶¶ 85–88. On the current record, Dr. Rubin fails to convince us of a material difference between the magnetic or optical disk, USB key drive, or other devices that he claims are long-term storage devices and the “data storage” in Foster’s PC. *See* Rubin Decl. ¶ 86 (citing Ex. 1001, 67:36–40). All are capable of long-term storage.

There is a further reason we do not agree with Patent Owner’s argument on this limitation at this stage. For this limitation Petitioner relies also on the disclosure of a storage device in Hayhurst. *See, e.g.*, Pet. 62–64 (arguing there is a motivation to combine Hayhurst’s storage with Foster’s encryption system). As discussed *supra*, Hayhurst’s decentralized media delivery system provides each user with subscriber device that includes a device for storing encrypted segments of media files. *See* discussion in Section I.H.3, *supra*. The subscriber units store these segments until they are requested in response to a request from one of the subscribers. Pet. 57–58 (citing Ex. 1007 ¶¶ 7, 28); *see also* discussion *supra* in Section I.H.3.

Patent Owner does not address this combination of Foster with the teachings of storage of digital information in Hayhurst. In particular, Patent Owner does not address the fact that on this record, Hayhurst’s storage of

encrypted segments of media files for distribution to subscribers would qualify as “long-term” storage, even under Patent Owner’s proposed construction.

For the reasons given, we determine that Petitioner has demonstrated sufficiently that this limitation is met by Foster and Hayhurst.

3. *“Plurality of Data Chunks” Limitation*

Claim 1 recites “distributing the data set into a plurality of data chunks” and “encrypting each of the data chunks with a respective one of a plurality of encryption keys.” Limitations IA, 1B. *supra*; claim 9 (Ex. 1001, 109:63–67).

Petitioner asserts that Foster’s encrypted payloads are the claimed “data chunks.” *See* Pet. 68–69. Patent Owner argues that Petitioner “has not, and cannot, demonstrate that the payloads of Foster’s content packets are ‘data chunks.’” Prelim. Resp. 29. According to Patent Owner, Foster’s payloads are not data chunks because they are “payloads of packets that arise as a result of transmission according to the MPEG video compression standard.” *Id.* at 30. Dr. Rubin testifies that “[t]he ’116 data chunks and Foster’s packets serve entirely different purposes.” Rubin Decl. ¶ 81. Patent Owner argues that by contrast, the purpose of generating the data chunks in the ’116 patent is to increase security. Prelim. Resp. 32.

At this stage, Patent Owner’s argument is unavailing. Patent Owner focuses on Foster individually, and does not address Hayhurst’s teaching and stated objective of a method to further secure the data. *See supra*, Section I.H.3; Ex. 1007 ¶ 2 (“This application relates to the field of electronic media delivery, . . . including the secure handling and storage of such media.”). For example, Petitioner explains that Hayhurst teaches that one of the benefits of segmenting and distributed storing of media-file segments, such

as Foster’s content units, is to provide “a high level of security and a deterrence to piracy.” *Id.* at 62 (quoting Ex. 1007 ¶ 8). Further, Petitioner’s rationale for combining the teachings of Foster and Hayhurst includes “increased security.” Pet. 64. We are not persuaded by Patent Owner’s assertion that “[a]dding Hayhurst to the combination [with Foster] cannot cure the fundamental difference” because it is without further explanation or record support. Prelim. Resp. 27.

At this stage and on this record, for the reasons given we disagree with Patent Owner’s argument based on alleged “fundamental differences” between Foster and the ’116 patent because it does not address Petitioner’s reliance on the teachings of Hayhurst in combination with Foster. *See* Prelim. Resp. 24–27. We find at this stage, for the reasons given that Petitioner demonstrates sufficiently that Foster combined with Hayhurst, teaches or suggests the “plurality of data chunks” limitation.

4. “Separately Storing” Limitation

Claim 1 recites “separately storing each data chunk of the plurality of data chunks.” Limitation 1D, *supra*. Claim 9 recites the identical limitation. Ex. 1001, 101:3–4. For this limitation, Petitioner cites the application of Hayhurst’s distributive storing techniques to the encrypted content units of Foster’s digital content. Pet. 72 (citing Bhattacharjee Decl. ¶ 263). Referring to Foster’s Figure 8, *supra*, Petitioner continues: “In Foster-Hayhurst, each encrypted content unit (i.e., processed content unit 116) is stored on a different Foster-Hayhurst subscriber unit, as taught by Hayhurst.” *Id.* at 73 (citations and internal quotation marks omitted).

Patent Owner responds that “[e]ven 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.” Prelim. Resp. 34. Patent Owner continues, “[i]n 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.” *Id.*

For the reasons given previously, at this stage we do not find this argument to be persuasive. *See* Section II.D.2, *supra*. First, we find that Petitioner has demonstrated sufficiently that Foster discloses the claimed storage devices. *See id.* In addition, Patent Owner fails to address the teachings of the Foster-Hayhurst combination. We determine that this combination meets this limitation, especially in light of Hayhurst’s disclosure of storage devices storing segments of one or more media files (e.g., movies). *See* discussion in Section I.H.3, *supra*.

In summary, we find at this stage for the reasons given that Petitioner demonstrates sufficiently that Foster, both alone and combined with Hayhurst, teaches or suggests the “separately storing” limitation.

5. *Summary and Conclusion – Foster-Hayhurst Ground*

We have considered Petitioner’s analysis of the Foster-Hayhurst ground and Patent Owner’s response. We determine that for the reasons given, Petitioner has demonstrated that there is a reasonable likelihood of prevailing on the Foster-Hayhurst challenge to independent claims 1 and 9. 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 and in the Petition, we determine also that Petitioner has demonstrated there is a reasonable likelihood of prevailing on the Foster-Hayhurst challenge to those claims. *See* Pet. 74–77.

III. CONCLUSION

Petitioner has shown a reasonable likelihood of prevailing as to the unpatentability of at least one challenged claim on at least one of its grounds. Patent Owner has not asserted any reason why we should exercise our discretion to deny institution of trial. Thus, we institute an *inter partes* review on all claims challenged in the Petition and on all grounds in the Petition.

IV. ORDER

It is

ORDERED that, under 35 U.S.C. § 314(a), an *inter partes* review of claims 1–3 and 5–14 of the ’116 patent is instituted for all grounds in the Petition; and

FURTHER ORDERED that, under 35 U.S.C. § 314(a), *inter partes* review of the ’116 patent is instituted on this Decision’s entry date, and under 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is given of the trial’s institution.

IPR2024-00212
Patent 11,178,116 B2

FOR PETITIONER:

Elisabeth H. Hunt
Richard F. Giunta
Marc S. Johannes
Wolf, Greenfield & Sacks, P.C.
EHunt-PTAB@wolfgreenfield.com
RGiunta-PTAB@wolfgreenfield.com
MJohannes-PTAB@wolfgreenfield.com

FOR PATENT OWNER:

Stephen J. Elliott
Andrei Iancu
Sullivan & Cromwell LLP
elliotts@sullcrom.com
iancua@sullcrom.com

Kenneth Weatherwax
Lowenstein & Weatherwax LLP
weatherwax@lowensteinweatherwax.com