Trials@uspto.gov
571-272-7822

Paper 43
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.

---

IPR2024-00215
Patent 10,452,854 B2

---

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

REPKO, *Administrative Patent Judge*.

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

# I. INTRODUCTION

Google LLC ("Petitioner") filed a petition requesting *inter partes* review of claims 1–10 of U.S. Patent No. 10,452,854 B2 (Ex. 1001, "the '854 patent"). Paper 2 ("Pet."). Security First Innovations, LLC ("Patent Owner") filed a Preliminary Response. Paper 9 ("Prelim. Resp."). On May 31, 2024, the Board instituted an *inter partes* review of all challenged claims based on all grounds in the Petition. Paper 15 ("Inst. Dec.").

Patent Owner filed a Response to the Petition. Paper 21 ("PO Resp."). Petitioner filed a Reply. Paper 24 ("Reply"). Patent Owner filed a Sur-reply. Paper 32 ("Sur-reply"). An oral hearing for this case was held on February 27, 2025. Paper 25.

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued under 35 U.S.C. § 318(a). For the reasons that follow, Petitioner has proved by a preponderance of the evidence that claims 1–10 are unpatentable.

## *A. Related Matters*

According to the parties, the '854 patent has been asserted in *Security First Innovations, LLC v. Google LLC*, No. 2:23-cv-00097 (E.D. Va.) (transferred from Alexandria Division, 1:23-cv-00329). Pet. xi; Paper 6, 1 (First Updated Mandatory Notices). Patent Owner further indicates that IPR2024-00212, IPR2024-00213, and IPR2024-00214 are related administrative matters. Paper 6, 1. The Board denied institution in IPR2024-00213. *See* IPR2024-00213, Paper 8.

### *B. The '854 Patent*

The '854 patent generally relates to securing data from unauthorized access or use. Ex. 1001, 1:25–26. The data to be secured is parsed, split, or separated into several parts. *Id.* at 2:47–49. The data is encrypted either before or after the parsing, splitting, or separating. *Id.* at 2:49–52. The encryption step can be repeated. *Id.* at 2:52–54.

In one embodiment, the '854 patent describes a fault-tolerant scheme for disaster recovery. *Id.* at 70:26–39. This scheme allows the original data to be regenerated from a subset of all data chunks. *See, e.g.*, *id.* For example, the data can be divided into four portions and stored in four different locations. *Id.* at 70:33–38. To successfully recreate the original data, the fault-tolerant scheme needs only two of the four portions. *Id.* This is beneficial if the data at two locations is lost or otherwise corrupted. *Id.* Also, the fault-tolerant feature can be used to implement the "two-man rule," in which two entities need to combine their portions to retrieve the original data. *Id.* at 70:40–47.

### *C. Claims*

Of the challenged claims, only claim 1 is independent.

1. A method for securely storing a data set, the method comprising:

    receiving an external key from an external storage system,

    generating a plurality of data chunks based on the data set, such that the data set can be reconstructed using at least a minimum number of the plurality of data chunks, wherein generating the data chunks comprises:

distributing the data set into a plurality of shares, wherein each of the shares comprises less than all of the data set,

accessing a plurality of distinct encryption keys,

encrypting each of the shares with a respective one of the plurality of distinct encryption keys,

performing an encryption operation based on the external key to further secure the plurality of data chunks; and

storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different storage devices.

*Id.* at 83:19–36.

### *D. Evidence*

| Name | Reference | Exhibit No. |
|---|---|---|
| Orsini | US 2004/0049687 A1, published Mar. 11, 2004 | 1005 |
| Foster | US 2003/0200176 A1, published Oct. 23, 2003 | 1006 |
| Hayhurst | US 2004/0216164 A1, published Oct. 28, 2004 | 1007 |

### *E. Asserted Grounds*

Petitioner asserts that claims 1–10 are unpatentable on the following grounds. Pet. 3.

| Claims Challenged | Pre-AIA[1] 35 U.S.C. § | Reference(s)/Basis |
|---|---|---|
| 1–10 | 102 | Orsini |
| 1–10 | 103(a) | Orsini |
| 1–10 | 103(a) | Foster, Hayhurst |

### *F. Dr. Bhattacharjee's Reply Declaration*

Petitioner submitted the Declaration of Samarat Bhattacharjee, Ph.D. with its Petition. Ex. 1003. During trial, Petitioner submitted a Reply Declaration from Dr. Bhattacharjee. Ex. 1111.

Patent Owner argues that the Board should disregard the Reply Declaration because Petitioner improperly incorporates it by reference. Sur-reply 1–2. According to Patent Owner, the Reply includes unexplained citations to forty-three new exhibits. *Id.* at 2 (citing Reply 9).

Patent Owner has not provided a sufficient reason for disregarding the entire Reply Declaration. *See id.* at 1–2. Patent Owner notes that the declaration is 256 paragraphs. *Id.* at 1. But our rules place no page limit on declarations. Also, Patent Owner has not submitted a motion to strike the declaration.

Even so, "[a]rguments must not be incorporated by reference from one document into another document." 37 C.F.R. § 42.6 (a)(3). The PTAB

[1] Petitioner asserts 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"). Pet. 3. Here, we apply the pre-AIA versions of 35 U.S.C. §§ 102 and 103.

Consolidated Trial Practice Guide (Nov. 2019) ("Trial Practice Guide")[2] provides guidance on incorporation by reference: "parties 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 (emphasis added). According to the Practice Guide, "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 the 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 id.* at 74–75.

## II. ANALYSIS

### *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. 6 (citing Ex. 1003 ¶¶ 37–38). Petitioner also asserts that a "higher level of education may substitute for less experience." *Id.*

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

In our Decision on Institution, we applied this definition. Inst. Dec. 4. Patent Owner submitted the Declaration of Dr. Rubin in support of its Response, and in that Declaration, Dr. Rubin accepted Petitioner's definition. Ex. 2033 ¶¶ 20–21. For the reasons given, we apply the same level of ordinary skill in the art that we did in the Institution Decision. Inst. Dec. 4.

### *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)).

In the Institution Decision, we construed claim 1 such that the external key can be received before or after the data chunks are generated. Inst. Dec. 9. We construed the recited data-set reconstruction. *Id.* at 11. And we provided guidance on the term "storage devices." *See id.* at 12 (commenting that we did not see support for limiting the term "storage

devices" to "long-term storage"). None of these constructions are at issue post-institution.

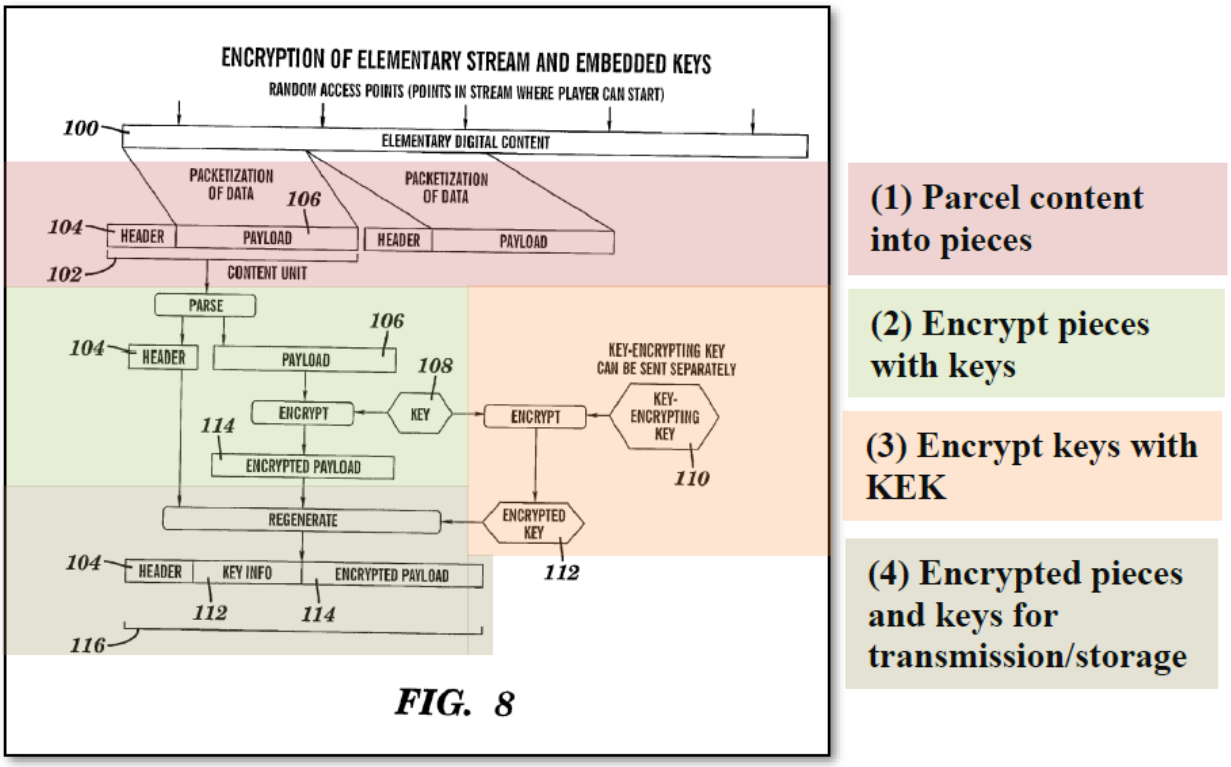
Neither party explicitly proposed constructions during trial, and we do not see the need for construing any terms in this Decision.

### *C. Obviousness over Foster and Hayhurst*

Petitioner asserts that claims 1–10 are unpatentable as obvious over Foster and Hayhurst. Pet. 55–89.

#### *1. Foster*

Foster's system encrypts streaming content before transmitting it. Ex. 1006 ¶ 2. Foster's Figure 8 is reproduced below with Petitioner's annotations. Pet. 56.



Petitioner annotates Figure 8 with labels on four different parts of Foster's method: (1) parceling elementary digital content 100 into content units 102 containing header 104 and payload 106, (2) encrypting payload 106 with key 108, (3) encrypting key 108 with key-encrypting key (KEK) 110 to create encrypted key 112, and (4) using encrypted key 112 to regenerate header 104, key info 112, and encrypted payload 114. *Id.*; *see also* Ex. 1006 ¶ 64.

### *2. 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. *Id.* ¶ 6. When a subscriber unit requests a media file, another subscriber unit encrypts the file segments that it has and forwards them to the requesting subscriber. *Id.* ¶ 7. 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 all segments of the media file. *Id.* ¶ 8. Also, storing the segments on multiple subscriber units provides redundancy when one subscriber unit cannot provide a segment. *Id.* ¶ 9.

### *3. Claim 1*

#### *a. Analogous Art*

"To be considered within the prior art for purposes of the obviousness analysis, a reference must be analogous." *Circuit Check Inc. v. QXQ Inc.*, 795 F.3d 1331, 1335 (Fed. Cir. 2015) (citing *Wang Lab. v. Toshiba Corp.*, 993 F.2d 858, 864 (Fed. Cir. 1993)). "Two separate tests define the scope of analogous prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the

field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved." *Sanofi-Aventis Deutschland Gmbh v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1377 (Fed. Cir. 2023) (quoting *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004) (citations omitted)).

*i. Petitioner's Burden*

Patent Owner argues that "Petitioner has the burden of proving Hayhurst is analogous art and did not attempt to carry that burden *in the Petition*." Sur-reply 2 (emphasis added); PO Resp. 32 ("Petitioner fails to prove Hayhurst is analogous art."). According to Patent Owner, "Petitioner makes no attempt to show that Hayhurst and the '854 [patent] share the same field of endeavor" (PO Resp. 33), and "Petitioner does not attempt to meet its burden of establishing that Hayhurst is reasonably pertinent because the Petition does not identify the problems [that Hayhurst or the '854 patent] are directed to, let alone compare them" (*id.* at 38).

But "[a] petitioner is not required to anticipate and raise analogous art arguments in its petition; instead a petitioner can use its reply to respond to" analogous art arguments raised by Patent Owner. *Sanofi-Aventis*, 66 F.4th at 1379 (citing 37 C.F.R. § 42.33), *cited in* Reply 2 n.2. Here, Petitioner used the Reply to respond to Patent Owner's analogous art arguments. *See* Reply 2–6. For the reasons in the sections that follow, Petitioner's reply arguments are persuasive. Thus, we disagree with Patent Owner's argument that the Foster-Hayhurst ground is deficient because Petitioner failed to meet its burden with respect to showing that Hayhurst is analogous art.
*See* PO Resp. 32–33, 38; Sur-reply 2.

*ii. Field of Endeavor*

In Patent Owner's view, the '854 patent's field of endeavor is securing data, and Hayhurst's is decentralized media delivery. PO Resp. 33; Sur-reply 3. Patent Owner argues that its view is supported by the title, abstract, figures, claims, and detailed description of the '854 patent and Hayhurst. *See* PO Resp. 34–36; Sur-reply 3.

Hayhurst's *Technical Field* section states,

> This application relates to the field of electronic media delivery, such as video-on-demand, including *the secure handling* and storage of such media.

Ex. 1007 ¶ 2 (emphasis added). That is, Hayhurst expressly states that the technical field includes secure handling of media. Reply 2 (quoting Ex. 1007 ¶ 2). There is no dispute that Hayhurst's media is data. *See* Tr. 78:4–19. Thus, Patent Owner's arguments contradict Hayhurst's *Technical Field* section.

Hayhurst's *Summary of the Invention* section mentions two security measures: segmentation and encryption. *See* Ex. 1007 ¶¶ 7, 8. On segmentation, Hayhurst states, "The segmented and distributed storage of the media file provides a high level of security and a deterrence to piracy." *Id.* ¶ 8, *cited in* Reply 2; *see also* Pet. 62 (discussing this paragraph). As for encryption, Hayhurst uses it to secure the segments. *See, e.g.*, Ex. 1007 ¶ 7.

Hayhurst's title is "Decentralized Media Delivery." *Id.,* code (54). Likewise, Hayhurst's abstract discusses segmentation and the "decentralized approach," which provide security *Id.*, Abst. Hayhurst's segmentation is an anti-piracy measure because, under this approach, each subscriber "will store only very small portions of the movie on the storage device of the unit." *Id.*

¶ 21. Thus, all the parts of Hayhurst identified in Patent Owner's table describe features that secure data. PO Resp. 35–36.

Patent Owner argues that Hayhurst's teachings are tangentially related to the security field because Hayhurst never says that the prior-art system needs better security. PO Resp. 36; *see also* Reply 2–3 (arguing security is a by-product in Hayhurst). According to Patent Owner, Hayhurst mentions secure handling and storage, but merely mentioning those features does not alter or expand its field to encompass the data-security field. PO Resp. 37. Patent Owner analogizes the situation here to the ones in *Wang Laboratories, Inc. v. Toshiba Corp.*, 993 F.2d 858, 864–65 (Fed. Cir. 1993) and *In re Clay*, 966 F.2d 656, 658–59 (Fed. Cir. 1992). *Id.* at 36–37. Patent Owner views these cases as confirming "that even art with some overlapping disclosures and in the same technological area as the subject patent may not be in the same field of endeavor." *Id.* at 36.

This case is factually distinguishable from *Wang Laboratories* and *Clay* because Hayhurst is very attuned to the relevant field of endeavor. *Id.* at 36–37. For instance, Hayhurst mentions security in the *Technical Field* section and two security measures in the *Summary of the Invention*. Ex. 1007 ¶¶ 2, 7, 8. Hayhurst repeats the piracy issue in both the *Summary of the Invention* section (*id.* ¶ 8) and the *Best Modes for Carrying Out the Invention* section (*id.* ¶ 21). Also, Hayhurst's repeated discussion of anti-piracy measures indicates that security is not merely a by-product, as Patent Owner argues (*see* Sur-reply 3–4).

Considering all the relevant parts of Hayhurst, we determine that Hayhurst and the '854 patent share the same field of endeavor: securing data. Thus, Hayhurst is analogous art.

*iii. Reasonable Pertinence*

Apart from being in the same field of endeavor, Hayhurst is analogous art because it is reasonably pertinent to the problem that the inventors were trying to solve. "Although the dividing line between reasonable pertinence and less-than-reasonable pertinence is context dependent, it ultimately rests on the extent to which the reference of interest and the claimed invention relate to a similar problem or purpose." *Donner Tech., LLC v. Pro Stage Gear, LLC*, 979 F.3d 1353, 1359 (Fed. Cir. 2020). Thus, under the reasonable-pertinence test applied below, we identify the problems that Hayhurst and '854 patent relate to. *Id.*

*(a) Problem Identified by Patent Owner*

Patent Owner argues that Hayhurst is not reasonably pertinent to the problem that the inventors were trying to solve: providing a cryptographic system with user-independent security and mobile support. PO Resp. 38–39 (citing Ex. 2033 ¶ 106). In Patent Owner's view, Hayhurst addresses only the bandwidth requirements of delivering video on demand. *Id.* at 39–40 (citing Ex. 1007 ¶¶ 4–5); Sur-reply 4–5.

Here, Patent Owner focuses on a single, narrowly formulated problem for each reference. *See* PO Resp. 38–40; Sur-reply 4–5. But a reference may be "reasonably pertinent to *one or more* of the particular problems." *Donner Tech.*, 979 F.3d at 1359 (emphasis added).

*(b) Problems Identified by Petitioner*

We agree with Petitioner that the '854 patent and Hayhurst are reasonably pertinent to several problems, including (1) user-independent security, (2) network security, and (3) distributed storage. *See* Reply 5–9.

*(1) User-Independent Security*

User-independent security is part of Patent Owner's formulation of the problem to be solved by the claimed invention. PO Resp. 38–39. Petitioner argues that Hayhurst is also related to user-independent security because it segments and distributes data without user interaction. *Id.* at 5 (citing Ex. 1007 ¶ 27). We agree because Hayhurst characterizes the distribution and storage as being automatic. Ex. 1007 ¶ 27. Hayhurst's segmentation and decentralized distribution provide security from piracy because each subscriber will store only a small part of the movie. *See* Section II.C.3.a.ii *infra*; Ex. 1007 ¶ 21. That is, no one subscriber can undermine the security scheme. Ex. 1007 ¶ 21. Thus, both Hayhurst and the claimed invention are reasonably pertinent to user-independent security.

*(2) Network Security*

As for network security, Petitioner argues that the '854 patent identifies the problem of ensuring that data is securely transmitted. Reply 5–6 (citing Ex. 1001, 1:30–39; Ex. 1009, 109–10). In Petitioner's view, Hayhurst also addresses secure data handling and deterring piracy. *Id.* at 6 (citing Ex. 1007 ¶¶ 2, 8). Petitioner's argument here is adequately supported by the record. For example, the '854 patent discusses data transmission in the first paragraph of the *Background of the Invention* section, calling secure transmission an "ever-increasing need." Ex. 1001, 1:30–39. Dr. Rubin testified that this is "part of the problem that the invention solves." Ex. 1009, 110:10–11.

Hayhurst's decentralized approach also ensures secure transmission. *See* Section II.C.3.a.ii *supra*. Although Dr. Rubin calls Hayhurst's security benefits "ancillary" (Ex. 2033 ¶¶ 108–109, *quoted in* PO Resp. 40), this does not align with Hayhurst (*see* Ex. 1007 ¶¶ 2, 7, 8, 21). For example, Hayhurst describes the security measures in the *Technical Field* section (*id.* ¶ 2) and the *Summary of the Invention* section (*id.* ¶¶ 7, 8). Hayhurst also discusses piracy deterrence in both the *Summary of the Invention* section (*id.* ¶ 8) and the invention's detailed description (*id.* ¶ 21). Because Dr. Rubin does not give sufficient weight to Hayhurst's discussion of piracy deterrence and security, we do not credit Dr. Rubin's testimony on this issue. *See* Ex. 2033 ¶¶ 108–109. Thus, we agree with Petitioner that Hayhurst is reasonably pertinent to the network-security problem that the inventors were trying to solve. *See* Reply 5–6.

*(3) Distributed Storage*

Distributed storage is the last of the three problems discussed by Petitioner. Reply 6. We agree that the '854 patent is concerned with solving this problem because the patent discusses measures to guard against any one data-storage facility being compromised. Ex. 1001, 56:47–50. For example, the '854 patent splits the encrypted file into shares and stores them in different locations. *Id.* The data-storage facilities can be "geographically remote." *Id.* at 5:53–56. Hayhurst also describes a segmented and decentralized approach to storing data. *See* Section II.C.3.a.ii *supra*. Thus, we agree with Petitioner that Hayhurst is reasonably pertinent to the distributed-storage problem that the inventors were trying to solve. *See* Reply 6.

*(c) Conclusion*

In sum, Hayhurst is reasonably pertinent to the particular problems with which the inventor is involved: (1) user-independent security, (2) network security, and (3) distributed storage. For this additional reason, Hayhurst is analogous art. *See* Section II.C.3.a.ii *supra* (explaining why Petitioner has shown that Hayhurst is in the '854 patent's field of endeavor).

*b. Receiving the External Key and Generating the Data Chunks*

Claim 1 recites, in part,

> A method for securely storing a data set, the method comprising:
>
> > generating a plurality of data chunks based on the data set, . . . wherein generating the data chunks comprises: distributing the data set into a plurality of shares, wherein each of the shares comprises less than all of the data set . . . .

Ex. 1001, 83:22–24.

Petitioner asserts that Foster's system generates a "plurality of data chunks based on the data set," as claimed, because it generates encrypted payloads (the claimed "data chunks") by encrypting payloads of digital content (the claimed "data set"). *Id.* at 72. Petitioner annotates Foster's

Figure 8, below, to illustrate this argument. *Id.*

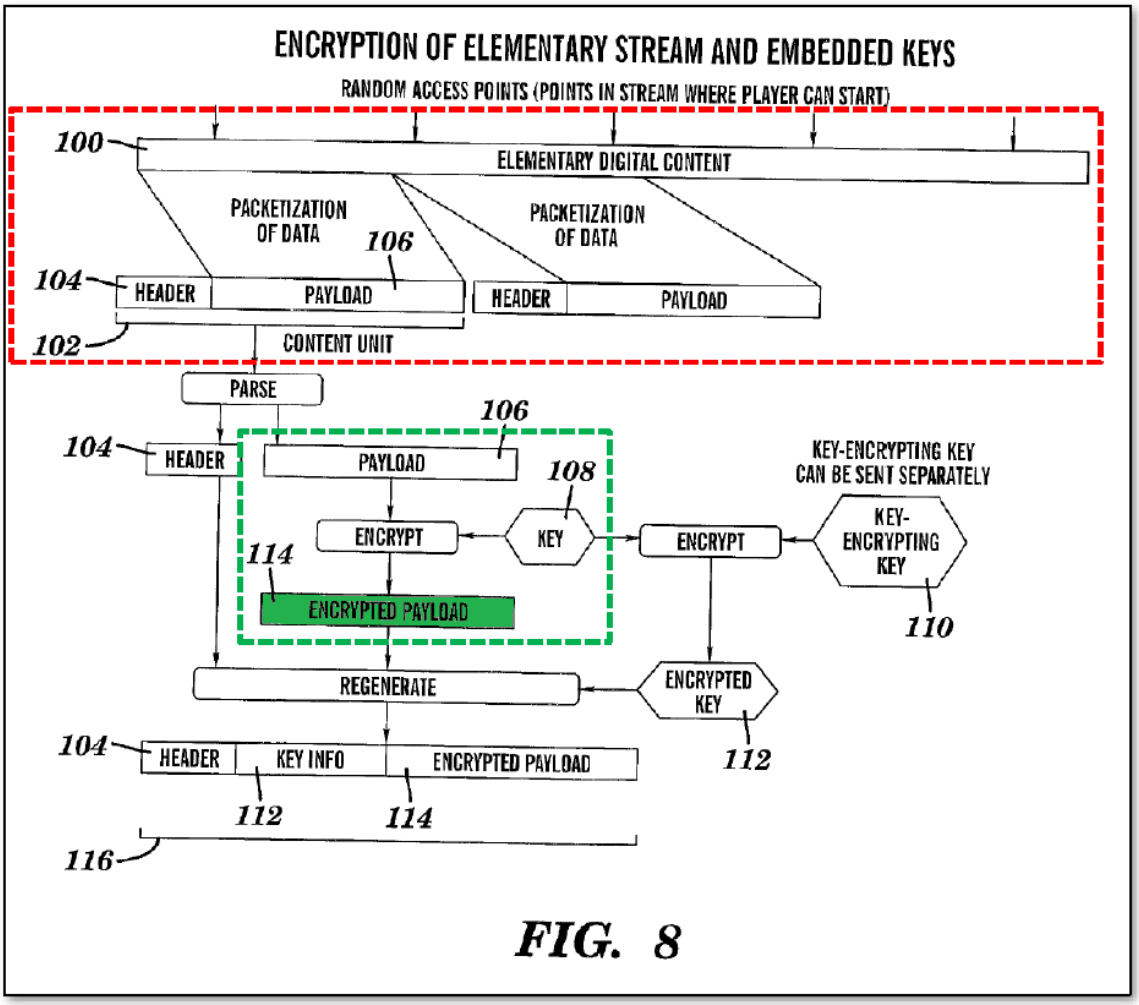



*FIG. 8*

Petitioner adds a red box around Foster's data packetization. *Id.* According to the Petition, the elementary digital content stream corresponds to the claimed "data set." *Id.* at 71 (citing Ex. 1003 ¶¶ 201–202). Elementary digital content 100 is packetized to create content unit 102. Ex. 1006 ¶ 64. Content unit 102 contains header 104 and payload 106. *Id.* After parsing, the system encrypts payload 106 using tile key 108 to create encrypted payload 114. *Id.* Under Petitioner's theory, payload 106 corresponds to the claimed "shares" (Pet. 74), and encrypted payload 114 (green fill) corresponds to the claimed "data chunks" (*id.* at 72).

*i. Data Chunks*

Claim 1 recites that "the data set can be reconstructed using at least a minimum number of the plurality of data chunks." Ex. 1001, 83:23–24.[3] Petitioner's challenge is based on the parties' proposed district court constructions for "data set." *See* Pet. 65–66. But neither party proposes a construction for "shares" or "chunks" in this proceeding. Even so, the meaning of "shares" and "data chunks" are readily apparent from the plain language: the data chunks are generated "based on the data set," and the claim defines the steps that comprise the chunk generation, including the relationship between the shares and the data set. *See* Ex. 1001, 83:19–31.

Patent Owner argues that Petitioner has not explained why Foster's payloads are shares or why its encrypted content units are data chunks. PO Resp. 63–64 (citing Pet. 72–74; Ex. 2033 ¶ 145). In Patent Owner's view, the Board should reject the Foster-Hayhurst ground because Petitioner's reasoning about the claimed shares and chunks is conclusory. *Id.* at 66.

We disagree. Rather, Petitioner explains that Foster teaches a data set:

> Foster's digital content is a "data set" under both parties' constructions because POSAs understood that, e.g., a video+audio data file is a "collection of related information made up of separate elements [e.g., video frames and audio samples] that can be treated as a unit [e.g., a file] in data handling"

[3] In the Institution Decision, we construed "the data set can be reconstructed using at least a minimum number of the plurality of data chunks" to encompass reconstructing the data set from all data chunks, but the claim is not limited to "a predefined number" of data chunks or reconstructing the data set with fewer than all data chunks. Inst. Dec. 12. The parties have not argued for an alternative construction. *See* PO Resp.; Reply; Sur-reply. The issues during trial do not turn on this construction.

> (Google; [Ex. 1064, 9–10]) and "a collection of information for storage" (SFI; [Ex. 1065, 6–7]).

Pet. 65–66 (citing Ex. 1003 ¶ 192). Petitioner also sufficiently explains why Foster's payloads (the "shares") satisfy the claimed relationship to the data set:

> As Foster's Figure 8 illustrates, each payload "*comprises less than all of the data set*," as claimed, because Foster discloses the entire stream ("*data set*") cannot be recovered from any one single payload.

Pet. 74 (citing Ex. 1006 ¶ 71; Ex. 1003 ¶ 212). Petitioner shows that Foster's elementary content stream ("data set") can be reconstructed using at least a minimum number of the plurality of content packets ("data chunks") for at least the reason that Foster uses all the encrypted packets to reconstruct the entire stream. Pet. 73 (citing Ex. 1006 ¶ 71). In this way, Petitioner sufficiently explains why Foster's payloads are shares and its encrypted content units are data chunks (Pet. 73), contrary to Patent Owner's argument (PO Resp. 63–64).

Patent Owner does not dispute that Foster's payloads are generated from and are a part of the content, as recited in claim 1. *See* PO Resp.; Sur-reply. Rather, Patent Owner argues for additional unrecited limitations to the terms "shares" and "chunks." *See* PO Resp. 66–68. For instance, Patent Owner argues that, in the '854 patent, packets are parsed into chunks but are not chunks themselves. *Id.* at 67–69 (citing Ex. 2033 ¶¶ 149–151); Sur-reply 17.

We see no reason for imposing this additional limitation. The '854 patent explains that a "wide number of alternatives" for data splitting can be used and that there is no limit to the size of the splitting, for example. Ex. 1001, 21:9–25, *cited in* Reply 14–15. In fact, any "suitable parsing and

splitting approach may be used to generate portions of data from an original data set," including randomly splitting. *Id.* at 74:56–75:10, *cited in* Reply 15.

Like the '854 patent's discussion of splitting data, Dr. Rubin's testimony indicates that splitting is relevant—but the particular method for doing so is not. *See* Ex. 1001, 21:9–25; 21:27–37; 74:56–75:10, *cited in* Reply 14–15. Specifically, Dr. Rubin testified that "the share is *the thing* that something gets split into" (Ex. 1099, 17:13–14) (emphasis added) and data chunks and shares are "*pieces* that have been split off from the original data set" (*id.* at 158:17–19) (emphasis added). We emphasize "the thing" and "pieces" here because those generic terms support our conclusion that a chunk should not be defined by the type of information that is split (e.g., packets). In view of Dr. Rubin's testimony and the '854 patent, we decline to read into the claim the additional unrecited limitations that Patent Owner argues for. *See* PO Resp. 66–68.

Consistent with the '854 patent (*see e.g.*, Ex. 1001, 21:9–25) and Dr. Rubin's testimony about shares and chunks (Ex. 1099, 17:13–14, 158:17–19), the Petition shows that Foster's encrypted payloads ("data chunks") are split off from the complete data set, as shown in Figure 8. *See* Pet. 71–74. In this way, Foster's encrypted payloads are generated "based on the data set." *See id.* Under Petitioner's theory, Foster distributes the data set into a plurality of shares because payload 106 corresponds to the claimed "shares" (*id.* at 74), which are related to the encrypted payload 114 (*id.* at 72) as claimed. *See* Ex. 1001, 83:19–31.

Dr. Rubin presents a selection of technical articles that use the terms "packet," "shares," and "chunks," and from this, Patent Owner concludes

that there is no reason to assume that Foster's encrypted payload[4] is a chunk. PO Resp. 66–67 (citing Ex. 2033 ¶ 147); Sur-reply 19. According to Dr. Rubin, numerous technical articles refer to a packet or packet payload as something that is divided into chunks or shares. Ex. 2033 ¶ 147 (citing Ex. 1042, 9; Ex. 2012, 3; Ex. 2013, 3; Ex. 2036, 1202; Ex. 2037, 1–2; Ex. 2038, 4–5; Ex. 2041, 7; Ex. 2043, 9532). Patent Owner argues that "Petitioner fails to provide any evidence showing that an MPEG packet/payload or any other type of packet/payload is terminology used to refer to a share/chunk." Sur-reply 19.

Although Foster calls subsets of data "payloads" instead of "shares" (*id.*), the prior art need not use the same words as the patentee. *See* Reply 16 (citing *Teva Pharm. Indus. Ltd. v. AstraZeneca Pharms. LP*, 661 F.3d 1378, 1384 (Fed. Cir. 2011)). As for Patent Owner's selection of technical articles, extrinsic evidence is "unlikely to result in a reliable interpretation of patent claim scope unless considered in the context of the intrinsic evidence." *Phillips*, 415 F.3d at 1318–19. Here, Patent Owner's extrinsic evidence is inconsistent with the specification because the '854 patent describes generating chunks from a wide variety of splitting and parsing techniques. *See* Ex. 1001, 21:9–25; 15:51–16:3, 21:27–37; 74:56–75:10. Thus, considering the context in which the '854 patent uses the terms, we see no reason to limit claim 1 to a particular splitting technique, such as dividing

[4] Patent Owner acknowledges that Petitioner maps Foster's encrypted payload 114 to the recited "data chunks." *See, e.g.*, PO Resp. 63. Dr. Rubin does too. Ex. 2033 ¶ 147. Even so, Patent Owner refers to "packet payloads," instead of *encrypted* payloads, in some parts of its Response. *See, e.g.*, PO Resp. 66. In those parts, we understand Patent Owner to mean encrypted payload 114.

the data set into packets and further dividing the packets into chunks or shares. *See* PO Resp. 66.

Patent Owner views Foster's reason for generating payloads as being significantly different from the invention's reason for generating the claimed chunks. *See* PO Resp. 68–69. Dr. Rubin characterizes Foster's payloads as merely a by-product of the MPEG standard existing at that time. Ex. 2033 ¶¶ 150–151. Patent Owner argues that, unlike Foster's payloads, the claimed invention generates data chunks to secure the data. PO Resp. 68–69 (citing Ex. 2033 ¶ 149); Sur-reply 17–18.

We rejected a similar argument in our Institution Decision (*see* Inst. Dec. 20–21), and nothing in the record developed during trial indicates that we should depart from our reasoning in that decision. Foster emphasizes the importance of securing the data set through encryption of pieces—that is, the content packets. *See* Ex. 1003 ¶ 4 (explaining the invention's objective). Although packetization is part of the MPEG standard (Sur-reply 18–19), Foster's packetization has separate advantages when combined with encryption: "it is not necessary for the same title key to be used to encrypt each content packet" because a different, encrypted title key can be attached to each packet. Ex. 1006 ¶ 65, *cited in* Pet. 77; *see also* Reply 15 (citing Ex. 1111 ¶ 147) (explaining how Foster's encryption works with the packet format). So, even assuming that the claim requires generating data chunks to secure the data, as Patent Owner argues (PO Resp. 68–69), Foster's stated goal is securing the digital content (Ex. 1003 ¶ 65), and the evidence supports Petitioner's argument that generating the encrypted payloads furthers that goal (Pet. 72–73; Reply 15–16). Thus, we credit Dr. Bhattacharjee's testimony about securing the data (Ex. 1003 ¶¶ 215–216) over Dr. Rubin's testimony on this issue

(Ex. 2033 ¶¶ 149–151) because Dr. Bhattacharjee's testimony is more consistent with Foster's disclosure of securing the content by encrypting the payload (*see* Ex. 1003, Fig. 8, ¶¶ 4, 65).

Thus, Petitioner has shown that Foster teaches or suggests the claimed data set, shares, and chunks.

*ii. Streaming*

*(a) Patent Owner's Arguments*

Patent Owner argues that a person of ordinary skill in the art would not have combined Foster and Hayhurst because they "are incompatible and have conflicting goals." PO Resp. 41. Patent Owner argues that Foster's goal is avoiding delays when streaming live television. *Id.* at 41–42; *see also id.* at 45–47 (discussing delays and latencies); Sur-reply 5–7 (same). For example, Patent Owner argues that Foster reduces video delay when a user changes the channel (PO Resp. 41–42) or when the user is viewing a live sporting event (*id.* at 45–47). In Patent Owner's view, Foster's solution is to synchronously transmit the encrypted packets with the corresponding encryption keys. *Id.* at 42–45.

Patent Owner argues that, unlike Foster, Hayhurst requires delays to receive and assemble a subscriber-requested movie. *Id.* at 47–49, 55–58; Sur-reply 6–7. According to Patent Owner, Hayhurst's distribution and storage method introduces delays that would prevent streaming or randomly accessing content, which obviates and contravenes Foster's goal. *See* PO Resp. 51–58; Sur-reply 6–7.

*(b) Foster's Storage Context*

Patent Owner's argument focuses on transmitting and streaming live events. *See* PO Resp. 41–58; Sur-reply 5–7. But the Petition relies on

Foster's teaching of storing encrypted content. *See, e.g.*, Pet. 65 (citing Ex. 1006 ¶ 8). Petitioner points this out in its Reply. *See* Reply 7–10. Patent Owner counters that Petitioner improperly shifts its unpatentability theory in the Reply because the Petition relies on Hayhurst's storage method, not Foster's storage context. Sur-reply 10–14. We disagree.

The Petition explicitly states that "Foster's method generates and *stores* a 'processed content unit 116.'" Pet. 80 (citing Ex. 1006 ¶¶ 65–66, 71) (emphasis added); *see also id.* at 57 ("the encrypted title key, encrypted content packet, and header are combined as a "processed content unit 116," which can be "*stored by a recipient*" (e.g., in a consumer's set-top box).") (emphasis added). Also, the Petition annotates Foster's Figure 8 with the text "(4) Encrypted pieces and keys for transmission/*storage*." *Id.* at 56 (emphasis added).

The Petition does not rely entirely on Hayhurst for the teaching of storing content at the receiver, as Patent Owner argues. *See, e.g.*, Sur-reply 13. Rather, the Petition relies on Hayhurst for multiple devices and analogizes Foster's recipient 430 to Hayhurst's subscriber units:

> POSAs had reason to store Foster's encrypted content units on multiple storage devices (*e.g.*, *consumer set-top boxes like Hayhurst's subscriber units and Foster's recipients 430*) based on Hayhurst's techniques for storing and distributing encrypted data segments.

Pet. 61 (emphasis added). In addressing the limitation on storage, Petitioner explains how Foster's receiver has a storage device:

> [Persons of ordinary skill in the art] understood such a receiver (e.g., consumer set-top box) includes a "*storage device*" ([Ex. 1006 ¶ 58] ("receiver may *cache*" (store) "KMBs…in *memory*" (a storage device)); also the combination's recipients are implemented with the functionality of Hayhurst's subscriber units, including their storage devices.

Pet. 80 (emphasis in original). Thus, the Petition clearly explains that the embodiment relied upon in Foster was the one that stores content at the receiver. *See id.* at 56, 57, 80.

In fact, our Institution Decision acknowledges Petitioner's reliance on Foster's storage context: "Petitioner argues that Foster's receiver 430 *stores* the data chunks in its storage device." Inst. Dec. 16 (citing Pet. 80) (emphasis added). On this issue, we preliminarily disagreed with Patent Owner's argument that Foster's receiver was not capable of storing content long term and that Foster's data set was not for storage. *See id.* 12, 16–18.

There is no dispute that Foster's receiver 430 can be a personal computer (PC) or set-top box. Foster describes how receiver 430 stores encrypted content. *See* Ex. 1006 ¶¶ 8, 79. For example, Foster explains, "Once received, recipient 430 can then synchronously store the encrypted content." *Id.* ¶ 79, *cited in* Pet. 68–69. According to Foster, "The 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), *quoted in* Pet. 65. In view of these parts of Foster, we credit Dr. Bhattacharjee's testimony that receiver 430 has data storage. Ex. 1003 ¶¶ 221–222.

*(c) Movie Distribution*

Although Patent Owner focuses on live television, the Petition relies on the embodiment in which users can "rent digital movies." Pet. 58–59 (citing Ex. 1003 ¶ 177); *see also id.* at 55 ("Foster's digital content includes '*any* data' (e.g., digital movie)") (quoting Ex. 1006 ¶ 37). In support of the Preliminary Response to the Petition, Patent Owner's declarant, Dr. Rubin,

acknowledged the movie embodiment by adding the words "Movie Studio" to Foster's Figure 16, as shown below. Ex. 2003 ¶ 83.

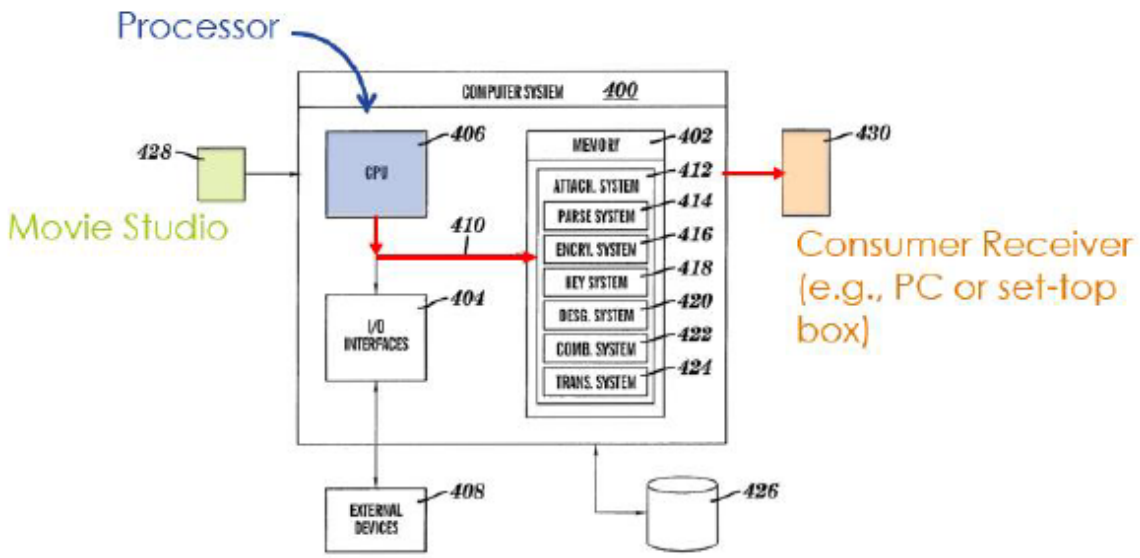



Figure 16, as annotated by Dr. Rubin, shows that the content is sent from movie studio 428 to receiver 43 via computer system 400. *Id.* According to the Petition, "The system also includes 'source 428' (green) which can be a 'content owner . . . such as a movie studio.'" Pet. 57 (citing Ex. 1006 ¶¶ 38, 42, 78). So although Patent Owner may have shifted its focus to other embodiments during trial, Petitioner's position has always been that Foster stores content, such as movies, at the receiver. *See id.*

Like Foster, Hayhurst distributes movies. *See* Ex. 1003 ¶ 23, *quoted in* Pet. 60. Patent Owner's arguments about changing channels (PO Resp. 41–42) and live sporting events (*id.* at 45–47) do not squarely address Petitioner's reasoning about how Foster's movie distribution could be improved by Hayhurst's technique (*see, e.g.*, Pet. 57–59). Foster's movie-distribution embodiment undermines the basic premise of Patent Owner's argument: the content distributed by Foster is very different from that of

Hayhurst. *See* PO Resp. 51–58; Sur-reply 6–7. To be sure, Foster's synchronization purportedly improves transmission (*id.*), but we disagree with Patent Owner's argument that improving transmission latency is the primary purpose. PO Resp. 41–42; *see also id.* at 45–47; Sur-reply 5–7. Rather, Foster expressly discloses that the synchronization method is applied in the storage context. Ex. 1006 ¶ 6.

*(d) DRMS and CAS*

In response to Patent Owner's characterization of Foster, Petitioner points to the background of Foster to show the types of systems that are in need of improvement. *See* Reply 8–9. For example, Petitioner identifies Foster's Figure 1, which is a flow diagram for a Digital Rights Management System (DRMS) that streams or stores content. *See id.* at 8 (citing Ex. 1006 ¶¶ 5, 49); 1006 ¶ 15. Figure 1 has the label "STREAMING OR STORED" between streaming media server 14 and PC 18. *See* Ex. 1006, Fig. 1.

Patent Owner acknowledges that Foster seeks to improve DRMS and CAS. *See* Sur-reply 7, 14–17. But Patent Owner characterizes Petitioner's reply argument as a new theory and argues that Petitioner essentially combines prior-art teachings with those of Foster's primary embodiment to arrive at a combination not presented in the Petition. *See id.* at 12–17.

Not so. Petitioner is merely arguing that Foster recognizes that synchronization can reduce latency in the storage context. Reply 8. We agree with Petitioner that Figure 1 supports this argument because DRMS, as described by Foster, involves packaging and storing content on a web server that is later downloaded and stored on a personal computer. *Id.* (citing Ex. 1006 ¶¶ 5, 49). In this way, Foster's discussion of improvements to

DRMS further bolsters Petitioner's argument that the benefits of Foster's synchronization are not limited to streaming live events. *See id.*

This is reflected in the Petition: Petitioner points out that Hayhurst improves Foster by "storing segmented content units on multiple devices in a distributed fashion." Pet. 62. Indeed, Hayhurst stores the data on the subscriber units to deter piracy—i.e., no single subscriber unit has all the segments for a complete media file. Ex. 1007 ¶ 8, *cited in* Pet. 59, 61. Also, because the segments are stored on multiple subscriber units, Hayhurst teaches that storing the content provides redundancy when one subscriber unit cannot provide a segment. *Id.* ¶ 9. We agree that Hayhurst's anti-piracy measures would only enhance Foster's objectives in the area of movie distribution. *See* Pet. 61–62. For this additional reason, Patent Owner's arguments that Foster and Hayhurst have conflicting goals (PO Resp. 52–55) or are incompatible (*id.* at 55–58) ignore the Petition's reliance on the storage context and movie distribution (*see, e.g.*, Pet. 58–59 (citing Ex. 1003 ¶ 177), 55 (quoting Ex. 1006 ¶ 37)).

Unlike Dr. Bhattacharjee's testimony, Dr. Rubin's testimony does not give sufficient weight to Foster's storage context and movie embodiments. *See* Ex. 2033 ¶¶ 127–134. Thus, we credit Dr. Bhattacharjee's testimony on the benefits to Foster's storage context (Ex. 1003 ¶¶ 182–190, 222) over Dr. Rubin's testimony on this issue (Ex. 2033 ¶¶ 127–134).

*iii. Drawbacks and Benefits*

Patent Owner argues that the combination's drawbacks outweigh its benefits. PO Resp. 61–62. According to Dr. Rubin, Foster has no need for Hayhurst's benefits: reduced bandwidth requirements, more security, and redundancy. *Id.* (quoting Ex. 2033 ¶¶ 139–141). Patent Owner argues that

any benefit would have been outweighed by the drawbacks, including delays that would have prevented random access to content and rendered live-television streaming impossible. *Id.* at 62 (Ex. 2033 ¶ 141); Sur-reply 6–7.

Having weighed the alleged drawbacks and benefits, we disagree with Patent Owner that one of ordinary skill in the art would not have made the combination.

*(a) Storage Context and Movie Embodiments*

Dr. Rubin does not give sufficient weight to Foster's storage context and movie embodiments. *See* Ex. 2033 ¶ 140; Section II.C.3.b.ii. *supra*. For example, Dr. Rubin testifies that "it would be more complicated to switch KEKs than in Foster alone as all of the content units are distributed across the subscribers *instead of streamed in real time* as in Foster." Ex. 2033 ¶ 148. Dr. Rubin repeatedly characterizes Foster as being focused on streaming (*see, e.g.*, *id.* ¶¶ 140, 148) and testifies that the combination would introduce "enormous delays" that would make it unsuitable for streaming live events (*id.* ¶ 141). But Petitioner relies on Foster's embodiment in which the receiver stores movies. *See* Pet. 56, 57, 80. That is, the drawbacks identified by Dr. Rubin do not apply to the combination proposed in the Petition because the combination is not based on the live-event streaming embodiment. *See id.* Thus, we credit Dr. Bhattacharjee's testimony on the benefits to Foster's storage context (Ex. 1003 ¶¶ 182–190, 222) over Dr. Rubin's testimony about streaming live events (Ex. 2033 ¶¶ 140–141, 148).

Dr. Rubin testifies that Foster does not indicate that it suffers from the bandwidth limitations comparable to Hayhurst's video-on-demand system. Ex. 2033 ¶ 140. Petitioner, though, points out that Foster's system also deals

with video-on-demand. Here again, Dr. Rubin does not give sufficient weight to the embodiment that Petitioner relies upon. *See* Ex. 2033 ¶ 140; Section II.C.3.b.ii. *supra*.

*(b) Foster's KEK*

Dr. Rubin also testifies that Foster's system has "sufficient security at the source" that would be undermined in the combination. Ex. 2033 ¶ 141. According to Dr. Rubin, the proposed combination would expose Foster's KEKs. Ex. 2033 ¶ 141. Patent Owner argues that the proposed combination would distribute Foster's KEKs across thousands of subscribers, making them more vulnerable and eliminating Foster's ability to change the KEKs. PO Resp. 58. Dr. Rubin testifies that Foster's KEKs are unique to each recipient and can be changed if compromised. *See* Ex. 2033 ¶¶ 135–136. In Patent Owner's view, these security features would be undermined by Petitioner's combination because distributing the content would increase the chances that the KEKs would be compromised. PO Resp. 59–62; Sur-reply 8–9. In Patent Owner's view, Petitioner's characterization of Foster's ability to change the KEKs is contradicted by the reference. Sur-reply 8 (citing Ex. 1006 ¶ 54; Ex. 2046, 25:21–27:10).

We are persuaded by Petitioner's reply arguments on this point. Reply 12–13. In particular, Petitioner points out that Patent Owner ignores the security benefits of Hayhurst's decentralized approach: "an attacker must collect chunks from Foster-Hayhurst's multiple storage devices, rather than from one storage device, as in Foster." *Id.* at 12 (citing Pet. 59–60; Ex. 1007 ¶¶ 5, 8). This is consistent with Hayhurst's disclosure:

> The segmented and distributed storage of the media file provides a high level of security and a deterrence to piracy. No single

> subscriber has more than a segment of a media file, which . . . by itself, has little value.

Ex. 1007 ¶ 8.

Likewise, Dr. Rubin does not give sufficient weight to Hayhurst's disclosure about each segment having little value itself. *See* Ex. 2033 ¶¶ 135–136, 141. Thus, we credit Dr. Bhattacharjee's testimony (Ex. 1003 ¶¶ 182–190, 222) over Dr. Rubin's testimony (Ex. 2033 ¶¶ 135–136, 141) on this issue.

*(c) Redundancy*

Patent Owner argues that Foster has no need for redundancy in the one-to-one basis because it can resend packets. PO Resp. 62. But Petitioner identifies an additional benefit to having redundant data sources that Patent Owner overlooks: Hayhurst's method allows the select a one or more data sources closer to the destination to deliver content faster than any one source may be able to achieve. Reply 13 (citing Ex. 1009, 89–92). This is corroborated by Dr. Rubin's testimony that servers could be located near places with high population density. Ex. 1009, 92:3–14.

*(d) Catastrophic Failures*

Patent Owner's arguments (PO Resp. 62) do not account for events that could affect the source's ability to resend send packets, such as a power or network failure (*see* Reply 13 (citing Ex. 1009, 135–37)). Petitioner's argument better aligns with Dr. Rubin's testimony in his deposition about how redundancy protects against catastrophic failure of a single machine. *See* Ex. 1009, 135–37.

*(e) Conclusion*

Even assuming that there would have been some reduction in security by distributing the KEK in the proposed combination, we agree with Petitioner that these concerns would not have outweighed the improvements in performance—that is, speed and efficiency. *See* Reply 13. But even the security concerns that are raised by Patent Owner (*see, e.g.*, PO Resp. 61–62; Sur-reply 8–9) would have been counterbalanced by the increase in security inherent in the distributed system and the limited value of compromising any single segment (Reply 12–13; Ex. 1007 ¶ 8).

*c. Remaining Limitations*

Apart from the arguments discussed above, Patent Owner does not present arguments specifically directed to the subject matter recited in the rest of the claim. *See* PO Resp. Even so, Petitioner has the burden to show that the challenged claims are unpatentable. Thus, we have reviewed Petitioner's arguments and evidence submitted in connection with the remaining limitations and conclude that Petitioner has shown that claim 1 is unpatentable over Foster and Hayhurst. *See* Pet. 55–82.

*4. Claims 2–10*

Petitioner contends that claims 2–10 are unpatentable over the Foster-Hayhurst combination. Pet. 82–89. Patent Owner does not present arguments specifically directed to claims 2–10. *See* PO Resp. Even so, Petitioner has the burden to show that the challenged claims are unpatentable. We have reviewed Petitioner's arguments made in connection with claims 2–10 and find them persuasive. *See* Pet. 82–89.

### *D. Anticipation and Obviousness over Orsini*

Petitioner asserts that claims 1–10 are unpatentable as anticipated by or obvious over Orsini. Pet. 8–54. Because we have determined that Petitioner has shown that claims 1–10 are unpatentable as obvious over the Foster-Hayhurst combination, we need not reach this ground. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359 (2018) (holding a petitioner "is entitled to a final written decision addressing all of the claims it has challenged"); *Boston Sci. Scimed, Inc. v. Cook Grp.*, 809 F. App'x 984, 990 (Fed. Cir. 2020) (non-precedential) (agreeing that the Board has "discretion to decline to decide additional instituted grounds once the petitioner has prevailed on all its challenged claims").

## III. CONCLUSION

Petitioner has proved that claims 1–10 are unpatentable by a preponderance of the evidence.[5]

| Claim(s) | 35 U.S.C. § | Reference(s)/ Basis | Claims Shown Unpatentable | Claims Not Shown Unpatentable |
|---|---|---|---|---|
| 1–10 | 102 | Orsini[6] | | |
| 1–10 | 103(a) | Orsini[7] | | |
| 1–10 | 103(a) | Foster, Hayhurst | 1–10 | |
| **Overall Outcome** | | | 1–10 | |

[5] 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).
[6] We need not reach this ground. *See* Section II.D *supra*.
[7] We need not reach this ground. *See* Section II.D *supra*.

## IV. ORDER

It is

ORDERED that Petitioner has proved by a preponderance of the evidence that claims 1–10 of the ’854 patent are unpatentable; and

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.

FOR PETITIONER:

Elisabeth H. Hunt
Gregory S. Nieberg
WOLF, GREENFIELD & SACKS, P.C.
ehunt-ptab@wolfgreenfield.com
gnieberg-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