

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX INC. AND HULU, LLC,
Petitioners,

v.

DIVX, LLC,
Patent Owner.

Case IPR2020-00558
Patent 10,225,588

**PATENT OWNER DIVX LLC'S RESPONSE
TO PETITION FOR INTER PARTES REVIEW
OF UNITED STATES PATENT NO. 10,225,588**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	PETITIONER FAILS TO SHOW THAT A POSITA WOULD BE MOTIVATED TO MODIFY CHEN TO INCOPORATE PARTIAL FRAME ENCRYPTION WITH A REASONABLE LIKEILHOOD OF SUCCESS.....	1
A.	For Multiple Reasons, The Petition Fails To Establish A Motivation To Combine Lindahl’s Partial Frame Encryption With Chen As A Matter Of Law.....	3
B.	Chen Improves Its Latency, User Experience And Efficiency Through Features That Are Incompatible, Or Beyond The Skills Of A POSITA To Implement, With Partial Frame Encryption.....	9
1.	Chen’s Independent Layers And Forward Error Correction Are Integral Features That Improve The Latency, User Experience, And “Efficiency” Of Its System.	11
2.	Implementing Partial Frame Encryption Together With Independent Scalable Layers And Forward Error Correction Presented Many Potentially Insurmountable Challenges Beyond The Skills Of A POSITA.	13
3.	A POSITA Would Not Have Been Motivated To Combine Chen And Lindahl Without Chen’s Integral Features Because That Would Reduce, Not Improve, Efficiency.	18
4.	The Need To Modify Standard File Formats Would Further Counsel A POSITA Against Combining Chen And Lindahl. .	22
III.	PETITIONER FAILS TO SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS “LOCATING ENCRYPTION INFORMATION...WITHIN THE REQUESTED PORTIONS OF THE SELECTED STREAM OF PROTECTED VIDEO” (ALL CLAIMS).....	24
A.	The Plain Meaning Of The Claims And Every Embodiment In The '588’s Specification Requires “Locating Encryption Information” “Within The Requested Portions Of The Selected Stream Of Protected Video.”	26
B.	Petitioner Fails To Prove That The Lindahl/Chen Combination Teaches Or Renders Obvious Locating Encryption Information Within Requested Portions Of The Selected Stream As Claimed.	35

C.	Petitioner Offers No Basis To Modify Lindahl To Disclose “Locating Encryption Information Within The Requested Portions Of The Selected Stream Of Protected Video.”	37
IV.	PETITIONER FAILS TO SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS VIDEO FRAMES IN ALTERNATIVE STREAMS “THAT ARE ENCRYPTED USING A SET OF COMMON KEYS” (ALL CLAIMS).....	38
A.	The Petition Fails To Show That Chen In View Of Lindahl Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.	39
1.	Lindahl Does Not Disclose A Streaming System With Alternate Streams Of The Same Content.....	39
2.	Lindahl Teaches Using A Global Key To Encrypt Some Metadata, Not Content.	43
3.	It Would Not Have Been Obvious To Modify Chen In View Of Lindahl To Encrypt Alternate Streams Of Protected Video With A Global Key.	47
B.	The Petition Fails To Show That Chen In View Of Hurst Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.	52
1.	Experts Agree That Hurst Itself Does Not Provide Motivation To Encrypt “Video Frames” Of Alternative Streams Using “A Set Of Common Keys.”	53
2.	The Petition’s Fails To Show Any Proper Motivation To Modify Chen In View Of Hurst.	54
V.	CONCLUSION	58

TABLE OF AUTHORITIES

Page(s)

COURT DECISIONS

<i>ActiveVideo Networks, Inc. v. Verizon Communs., Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	6
<i>Allergan, Inc. v. Sandoz Inc.</i> , 796 F.3d 1293 (Fed. Cir. 2015)	54
<i>Arendi S.A.R.L. v. Apple Inc.</i> , 832 F.3d 1355 (Fed. Cir. 2016)	51
<i>DSS Tech. Mgmt. v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	51
<i>In re Chaganti</i> , 554 Fed. Appx. 917 (Fed. Cir. 2014).....	56
<i>In re Dembiczak</i> , 175 F.3d 994 (Fed. Cir. 1999)	57
<i>In re Lee</i> , 277 F.3d 1338 (Fed. Cir. 2002)	57
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	5
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge, Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	4
<i>Kinetic Concepts, Inc. v. Smith & Nephew, Inc.</i> , 688 F.3d 1342 (Fed. Cir. 2012)	9
<i>Kingsley v. United States</i> , 24 Ct. Cl. 219 (1889 Ct. Cl.)	34
<i>KSR Int’l Corp. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007)	57
<i>Medrad, Inc. v. MRI Devices Corp.</i> , 401 F.3d 1313 (Fed. Cir. 2005)	27
<i>Nestle’s Food Co. v. United States</i> , 16 Ct. Cust. 451 (1929 Ct. Cust. App.)	34

<i>Nichia Corp. v. Everlight Ams., Inc.</i> , 855 F.3d 1328 (Fed. Cir. 2017), <i>cert. denied</i> , 139 S. Ct. 183 (2018).....	9
<i>Northern Telecom Ltd. v. Samsung Elecs. Co.</i> , 215 F.3d 1281 (Fed. Cir. 2000)	26
<i>Otsuka Pharm. Co. v. Sandoz, Inc.</i> , 678 F.3d 1280 (Fed. Cir. 2012)	57
<i>Quality Edge, Inc. v. Rollex Corp.</i> , 709 Fed. Appx. 1000 (Fed. Cir. 2017).....	34
<i>W.L. Gore v. Garlock, Inc.</i> , 721 F.2d 1540 (Fed. Cir. 1983)	57
AGENCY DECISIONS	
<i>Cisco Sys., Inc. v. C-Cation Techs., LLC</i> , IPR2014-00454, Paper 12 (PTAB Aug. 29, 2014) (informative).....	4, 38
<i>Kingston Tech. Co., Inc. v. Polaris Innovations Ltd.</i> , IPR2016-01622, Paper 7 (PTAB Feb. 15, 2017).....	56
<i>Microsoft Corp. v. IpLearn-Focus LLC</i> , IPR2015-00095, Paper 33 (PTAB Apr. 11, 2016)	37
<i>Toyota Motor Corp. v. Gen. Elec. Co.</i> , IPR2019-00016, Paper 7 (PTAB Apr. 22, 2017)	5
<i>Unified Patents Inc. v. GE Video Compression, LLC</i> , IPR2019-00659, Paper 7 (PTAB Aug. 1, 2019).....	5
<i>Volkswagen Group of Am., Inc. v. Velocity Patent LLC</i> , IPR2015-00276, Paper 8, 13 (PTAB June 1, 2015)	6
RULES, RULEMAKING, AND OTHER AGENCY AUTHORITIES	
37 C.F.R. § 42.6(a)(3).....	4
37 C.F.R. § 42.65(a)	49

EXHIBIT LIST	
2001	Reserved
2002	U.S. Patent No. 8,909,922
2003	Excerpts from U.S. Patent Application No. 14/564,003 File History [003 CON FH]
2004	U.S. Patent No. 9,247,311 [Patent from 12/8/14 Continuation]
2005	Excerpts from U.S. Patent Application No. 14/970,412 File History [412 CON FH]
2006	U.S. Patent No. 9,621,522 [Patent from 12/15/15 Continuation]
2007	Excerpts from U.S. Patent Application No. 15/481,340 File history [340 CON FH]
2008	U.S. Patent No. 10,244,272
2009	U.S. Patent No. 8,806,188 [Braness]
2010	Manning <i>et al.</i> , INTRODUCTION TO INFORMATION RETRIEVAL (2008) (excerpts) [Manning]
2011	US Pat. App. US2009/0290706A1 [Amini]
2012	Declaration of Seth Nielson, Ph.D. [Nielson Decl.]
2013	Deposition of Patrick McDaniel, Nov. 16, 2020, [McDaniel Depo.]
2014	Struck <i>et al.</i> , The Elements Of Style, 2005 [Struck & White]
2015	Garner, The Redbook Manual On Legal Style, 2003 [Garner]

2016	Andy Patrizio, Why the DVD Hack Was a Cinch, WIRED, November, 2, 1999, available at https://www.wired.com/1999/11/why-the-dvd-hack-was-a-cinch/ [Patrizio]
2017	About Bruce Schneier, Schneier on Security, available at https://www.schneier.com/blog/about/ [Schneier Blog]
2018	Bruce Schneier, Why Cryptography Is Harder Than It Looks, Counterpane Systems, 1997, available at http://www.firstnetsecurity.com/library/counterpane/whycrypto.pdf [Schneier]
2019	Kevin Henry et. al., An Overview of the Advanced Access Content System (AACs), available at http://cacr.uwaterloo.ca/techreports/2007/cacr2007-25.pdf [Henry]
2020	Free-to-view, Wikipedia, available at https://en.wikipedia.org/wiki/Free-to-view [Free-to-view]

I. INTRODUCTION

For the reasons set forth below, the Petition fails to demonstrate by a preponderance of the evidence that any of the challenged claims (1-24) are unpatentable.¹

II. PETITIONER FAILS TO SHOW THAT A POSITA WOULD BE MOTIVATED TO MODIFY CHEN TO INCORPORATE PARTIAL FRAME ENCRYPTION WITH A REASONABLE LIKEILHOOD OF SUCCESS.

The claims-at-issue require “protected video” that “includes partially encrypted frames.” Ex. 1001 [’588 Patent] cls. 1, 12; *see also* Ex. 2012 [Nielson Decl.] ¶ 46. The Petition admits that Chen does not disclose “partially encrypted frames,” believing Chen to “not require any particular DRM implementation.” Pet., 18. Petitioner instead relies on Lindahl for the alleged disclosure of “partially encrypted frames.” Pet., 29, 36 (relying on Lindahl for disclosure of “video frames contain encrypted portions and unencrypted portions of data”).

¹ The Petition asserts without evidence or argument that the ’588 patent cannot claim the benefit of the filing date of its provisional application, but this question irrelevant because all of the Petition’s “relied-upon references...are prior art regardless.” Pet., 11. This Response assumes, *arguendo*, that the relied-upon references are all prior art.

The Petition contends that a POSITA would have been motivated to combine “Chen’s adaptive streaming teachings with ... Lindahl’s DRM teachings, including partial encryption and key management.” Pet., 17. Petitioner argues that a POSITA would have been motivated to apply Lindahl’s partial frame encryption to Chen to “address piracy concerns and improve efficiency,” directing just one sentence to establish to the goals animating its proffered motivation:

A POSITA would have been motivated to apply Lindahl’s teachings to Chen *to address piracy concerns and improve efficiency*, which Chen also raises as a goal. Ex. 1003 [McDaniel Decl.] ¶¶ 115, 119-120.

Pet., 18-19.²

The Petition is incorrect on multiple grounds. Ex. 2012 [Nielson Decl.] ¶¶ 47-48. First, as discussed in Section II.A, *infra*, the Petition’s single sentence (quoted above) fails to demonstrate that a POSITA would be motivated to combine Lindahl’s partial frame encryption with Chen as a matter of law because (a) it is not supported by any evidence aside from improper incorporated-by-reference citations to Dr. McDaniel’s declaration; (b) its single-sentence, conclusory

² Petitioner also contends that alternative streaming and partial encryption is combinable (Pet., 19-20), but, the only proffered *goals* animating the motivation to combine Lindahl’s partial frame encryption with Chen is “to address piracy concerns and improve efficiency.”

statement of generic goals is insufficient to establish a motivation to combine as a matter of law; and (c) Petitioner's combination is based on the incorrect premise that Chen does not already have an encryption regime and Petitioner does not demonstrate that its proffered goals would be better achieved through its combination over Chen's existing system.

Second, Petitioner does not establish that partial frame encryption would be superior to "address piracy concerns and improve efficiency" in the context of Chen's adaptive streaming system. In fact, Chen has various features, such as independent layers and Forward Error Correction (FEC), that are integral to Chen's system, but are incompatible with partial frame encryption, or at least would be beyond the capability of the POSITA to implement with partial frame encryption. Consequently, Petitioner fails to prove that a POSITA would either be motivated to combine Lindahl's partial frame encryption with Chen's adaptive streaming system or could do so with a reasonable likelihood of success. Furthermore, to the extent these features of Chen are not implemented in a combined system, Chen's system would, in fact, deteriorate in efficiency, negating Petitioner's proffered goal.

A. For Multiple Reasons, The Petition Fails To Establish A Motivation To Combine Lindahl's Partial Frame Encryption With Chen As A Matter Of Law.

As discussed above, Petitioner contends that a POSITA would be motivated to combine Lindahl's partial frame encryption with Chen's adaptive streaming

system. Petitioner provides a lengthy discussion in favor of its combination but proffers only a single sentence statement of the alleged benefits attributable to combining Lindahl's partial frame encryption with Chen:

A POSITA would have been motivated to apply Lindahl's teachings to Chen *to address piracy concerns and improve efficiency*, which Chen also raises as a goal. Ex. 1003 [McDaniel Decl.] ¶¶ 115, 119-120.

Pet., 18-19. It is Petitioner's burden to prove a motivation to combine. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 1367-68 (Fed. Cir. 2016). Petitioner's one-sentence statement should be rejected for at least three reasons.

First, Petitioner's statement is not supported by *any* cognizable evidence. The Petition cites three paragraphs (that include over 600 words) from its expert declaration but neither quotes from nor even characterizes what is said therein. The Office's rules preclude such incorporation by reference. 37 C.F.R. § 42.6(a)(3) ("Arguments *must* not be incorporated by reference from one document into another document."). It is well-settled that unexplained citations to an expert declaration should be ignored. Consolidated Trial Practice Guide (Nov. 2019), 35-36 ("parties that incorporate expert testimony by reference in their petitions ... without providing explanation of such testimony risk having the testimony not considered by the Board."); *Cisco Sys., Inc. v. C-Cation Techs., LLC*, IPR2014-00454, Paper 12, 9-10 (PTAB Aug. 29, 2014) (informative) (citations to expert declaration to "support

conclusory statements for which the Petition does not otherwise provide an argument or explanation” is improper incorporation by reference that will not be considered).

Because Petitioner’s motivation is not supported by any evidence, it fails as a matter of law. *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.”).

Second, Petitioner’s one-sentence assurance that its proffered combination would “address piracy concerns and improve efficiency” is stated in such conclusory and generic manner that it fails to establish a motivation to combine as a matter of law. *Hulu LLC v. Sound View Innovations LLC*, IPR2018-00582, Paper 34 at 20-21 (PTAB Aug. 5, 2019) (informative) (rejecting combination where petitioner had not “adequately supported” why it would have been a “good idea” to modify references). Both the Board and the Federal Circuit routinely reject “efficiency” and similar conclusory assertions as legally sufficient motivation. *See, e.g., Toyota Motor Corp. v. Gen. Elec. Co.*, IPR2019-00016, Paper 7, 27 (PTAB Apr. 22, 2017) (rejecting rationale to make something “more efficient”); *Unified Patents Inc. v. GE Video Compression, LLC*, IPR2019-00659, Paper 7, 14 (PTAB Aug. 1, 2019) (rejecting desire “to increase coding efficiency” as “insufficient” and “divorced from the prior

art elements”); *Volkswagen Group of Am., Inc. v. Velocity Patent LLC*, IPR2015-00276, Paper 8, 13 (PTAB June 1, 2015) (rejecting rationale of “improving fuel efficiency”); *ActiveVideo Networks, Inc. v. Verizon Communs., Inc.*, 694 F.3d 1312, 1327-28 (Fed. Cir. 2012) (desire for “a system that was more efficient, cheaper, or you wanted a system that had more features, makes it more attractive to your customers” is insufficient).

Third, Petitioner’s proffered motivation—“to address piracy concerns and improve efficiency”—assumes that Chen “did not require any particular DRM implementation.” Pet., 18. In fact, Chen discloses fragment-level encryption: *“because encryption is being employed to encrypt each fragment or block separately, and thus the entire fragment or block needs to be received before it can be decrypted.”* Ex. 1006 [Chen] ¶ 522. Chen’s statement that, because of encryption, “the entire fragment or block needs to be received before it can be decrypted” informs a person of ordinary skill in the art (POSITA) that the entire fragment or block is encrypted as a singular unit. Ex. 2012 [Nielson Decl.] ¶¶ 49-50.³

Fragment-level encryption is not frame or partial-frame encryption as disclosed in Lindahl. In Chen, the media content is divided into “smaller pieces,

³ Chen uses fragment and block synonymously. Ex. 1006 [Chen] ¶ 74.

perhaps on the order of a few seconds each, to form segments.” Ex. 1006 [Chen] ¶ 63; *see also id.*, ¶¶ 153, 200-205, 293. Each segment constitutes a separate file. *Id.* (“Each segment may then be stored on a web server or CDN as a separate file.”); *see also id.*, ¶ 72 (“The terms ‘file’ and ‘segment’ are used synonymously in this document unless otherwise specified.”). At the time of the invention, each second of a movie contains roughly 25-60 frames; therefore, a segment file of a few seconds would contain about 75-180 frames. Ex. 2012 [Nielson Decl.] ¶ 51. Each segment in turn consists of one or more fragments of, *e.g.*, a half-second. *See e.g.*, Ex. 1006 [Chen] ¶ 147 (“Multiple fragments may be concatenated into a single segment ...”); ¶ 141 (“with 500 [millisecond] movie fragments”); Ex. 2013 [McDaniel Depo.] 108:5-9 (“encrypting a fragment could be performed at a larger granularity than a frame”); *see also id.*, 106:21-107:3. Thus, Chen’s fragments could include, for instance, on the order of 12 to the 30 frames.

Other aspects of Chen confirm that its encryption is not performed at a frame level—partial or otherwise—and is instead performed at the fragment level. For example, Fig. 9(a) of Chen depicts an example of Chen’s “metadata table 900,” which corresponds to the metadata provided in connection with each one of the one of plurality of “alternative streams.” Ex. 1006 [Chen] ¶ 218. As depicted in Fig. 9(a), reproduced below with highlighted annotations added, DRM and encryption

information is provided at a “presentation level” (*i.e.*, for each of the alternative streams), and does not provide for any frame specific encryption information:

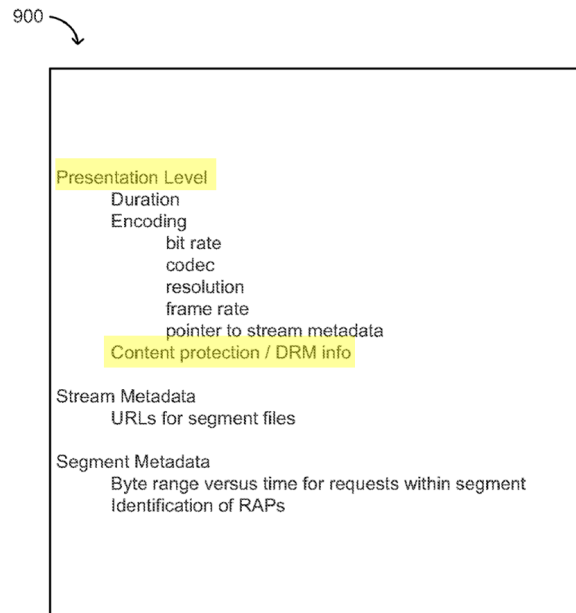


FIG. 9(a)

Ex. 1006 [Chen] Fig. 9(a); *see also id.*, ¶ 66 (“In particular, from the media presentation description, the HTTP streaming client may determine which segments in the collection can be accessed so that that the data is useful to the client capability and the user within the streaming service.”); Ex. 2012 [Nielson Decl.] ¶¶ 52-53.

Thus, Chen has a clear, fragment-level encryption system already. Petitioners do not identify any fault in Chen’s existing system, nor do they prove that replacing Chen’s encryption protocol with Lindahl’s partial frame encryption method would either “address piracy” or “improve efficiency” any better than Chen’s existing system already does. *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342,

1369 (Fed. Cir. 2012) (when two references “independently operate effectively” to accomplish similar functions, the POSITA “would have no reason” to combine them); *Nichia Corp. v. Everlight Ams., Inc.*, 855 F.3d 1328, 1339 (Fed. Cir. 2017), *cert. denied*, 139 S. Ct. 183 (2018) (that “references disclose different structures, resolve dissimilar problems, and propose dissimilar solutions” may be sufficient reason to reject proposed obviousness combination.). Even if the Board were to consider Dr. McDaniel’s improperly incorporated by reference paragraphs—which it should not—this testimony too does not explain why Lindahl’s approach is superior to Chen’s in terms of furthering Petitioner’s proffered goals. Ex. 1003 [McDaniel Decl.] ¶¶ 115, 119-120.

Consequently, Petitioner’s proffered motivation to combine fails as a matter of law.

B. Chen Improves Its Latency, User Experience And Efficiency Through Features That Are Incompatible, Or Beyond The Skills Of A POSITA To Implement, With Partial Frame Encryption.

As discussed in the preceding section, Petitioner generically contends that a POSITA would be motivated to add partial frame encryption to Chen’s system to “address piracy and improve efficiency.” Pet., 18. Petitioner’s argument, however, was premised on Chen not having an encryption protocol. Thus, Petitioner imagines that it is adding encryption to Chen as if Chen is a blank slate in this regard.

In fact, as discussed, Chen utilizes a fragment-based encryption protocol, and Petitioner fails to prove that a POSITA would have been motivated, or would have a reasonable expectation of success, to modify Chen to use (1) frame level encryption, (2) with partial frame encryption, (3) to “address[] piracy and improving efficiency.” Ex. 2012 [Nielson Decl.] ¶ 54.

Petitioner’s proposed combination of Lindahl’s partial frame encryption with Chen would face significant, potentially insurmountable hurdles, that Petitioner fails to address. As discussed in Section II.B.1, Chen’s adaptive streaming system relies upon certain integral features that improve latency, user experience, and efficiency. As discussed in Section II.B.2, however, Petitioner fails to explain how Chen’s integral features could be combinable with partial frame encryption or could be implemented with a reasonable likelihood of success. Moreover, if these features were excluded, the net result would be a significant *decrease* in efficiency without any improvement in “addressing piracy.” See Section II.B.3. A POSITA would also be mindful of other challenges, such as the fact that standard file formats contemplated in Chen were not compatible with partial frame encryption and had to be re-defined, all of which counsels against a motivation to combine. See Section II.B.4. Consequently, Petitioner fails to prove how its combination would further its alleged goals animating its combination or could be achieved with a reasonable likelihood of success.

1. Chen's Independent Layers And Forward Error Correction Are Integral Features That Improve The Latency, User Experience, And "Efficiency" Of Its System.

Chen discloses integral parts of its system that are central to its performance, user experience, and efficiency, as discussed in this sub-section, but that are incompatible or, at a minimum, very challenging to implement with partial frame encryption, as discussed in the following sub-section. Two such features in Chen, independent layers and Forward Error Correction, are discussed here.

One of the novel aspects of Chen's system that is used to improve Chen's efficiency, latency, and user experience is what it refers to as "independent scalability layers." Ex. 1006 [Chen] ¶ 27 ("In some embodiments, novel improvements to methods for encoding and decoding blocks with multiple independent scalability layers are provided."). This feature is so integral to Chen's performance that Chen is titled "Enhanced Block-Request Streaming ***Using Scalable Encoding***," (*id.*, Title), and all of Chen's claims require "scalable" video encoding technique (*id.*, cls. 1, 2). As Dr. Nielson explains:

Through this method, the information in a given segment or fragment is divided into multiple independent, parallel layers. *Id.*, ¶¶ 375-384; Fig. 12. Each layer would represent the same section of media, but is encoded differently such that the user can start playback after it has received a subset of the layers, and the quality of playback increases as the number of layers received by the user increases. *Id.*; see also Ex. 1006 [Chen] ¶ 381 ("[A] client that has received certain subset of the

layers may perform decoding and presentation of a representation of the content.”). This improves user experience and efficiency by allowing the user to receive as many layers of the content as the network bandwidth permits, without unnecessarily stalling while waiting to receive layers that the network cannot handle due to congestion. Ex. 1006 [Chen] ¶ 379.

Ex. 2012 [Nielson Decl.] ¶ 57; *see also id.*, ¶¶ 55-56; 58-60.

Forward Error Correction (FEC) is a second integral aspect of Chen’s system that is likewise used to improve Chen’s performance, latency and efficiency. As Dr. Nielson explains:

FEC is a technique wherein each packet of data includes certain information about subsequent packets. Ex. 1006 [Chen] ¶ 88. Through FEC, the already received packets can supplement or correct other packets that may have parts corrupted during transmission. Chen, however, utilizes FEC as an integral part of its system to enhance efficiency by “provide[ing] protection against long and variable delivery times of data ...” Ex. 1006 [Chen] ¶ 76; *id.*, (FEC “reduc[es] content zapping time and the variability in content zapping time.”). Chen utilizes FEC to permit its system to use already received packets to reconstruct packets that have not yet been received and start playing faster, thus improving timing performance by 70%. *Id.*, ¶¶ 529-533.

Ex. 2012 [Nielson Decl.] ¶ 61.

As will be discussed in the immediately following sub-section, the above described features of Chen are either incompatible with partial frame encryption or, at the very least, far beyond the skills of a POSITA to combine.

2. Implementing Partial Frame Encryption Together With Independent Scalable Layers And Forward Error Correction Presented Many Potentially Insurmountable Challenges Beyond The Skills Of A POSITA.

Implementing partial frame encryption, as the claim requires, together with Chen's independent scalable layers and FEC presents serious, potentially insurmountable hurdles that are, in any event, far beyond the skills of a POSITA to implement. Ex. 2012 [Nielson Decl.] ¶ 63.

As explained in the prior section, each fragment or segment (which includes multiple frames) in Chen is encoded as multiple scalable layers, and a user can reconstruct the requested video using only a subset of the layers. Ex. 1006 [Chen] ¶ 381. As Dr. Nielson explains, however, partial frame encryption is potentially incompatible with Chen's layer system insofar as the layer-system could compromise the encryption:

Chen's use of layers, however, is potentially incompatible with partial frame encryption because an unencrypted portion of one layer could be used to reconstruct the encrypted portion of a parallel layer, thus, compromising security. For example, as depicted below, an exemplary fragment in Chen has four layers, with red denoting encrypted portions and blue denoting unencrypted portions. Information in the encrypted

(red) portion of one layer may be determined from the information in the unencrypted (blue) portion of other layers:



For instance, if the client received both layers 2 and 4, the unencrypted portion of layer 2 could be used to fill in the encrypted portion of layer 4 and the unencrypted portion of layer 4 could be used to fill in the encrypted portion of layer 2. This would be a significant problem because it would mean that a client with no encryption key could still consume the encrypted portions of the media file. If unaddressed, this would not “address piracy,” it would aggravate security concerns.

Ex. 2012 [Neilson Decl.] ¶¶ 64-65.

Petitioner does not identify this disconnect much less address how a POSITA could resolve it. As Dr. Neilson explains, solutions to this problem are elusive:

Petitioner and Dr. McDaniel do not appear to explain how a POSITA could combine Lindahl’s partial frame encryption with Chen’s layers in a manner that preserves encryption and no obvious solutions are self-evident. For example, it would be impractical to attempt to encrypt identical segments of parallel layers because range of bytes in one layer does not correspond to the range of bytes in another layer and, therefore, it would be very difficult to create a system wherein only overlapping portions of layers are encrypted. *See also* Ex. 1006 [Chen] ¶ 135 (“fragments are not aligned between the different rate streams.”).

But even if all corresponding sections in different layers are encrypted, but other parts of the layers are not encrypted, it may still be possible to “infer” the encrypted data from the unencrypted portions of other layers. For example, “Temporal Scalability” (Ex. 1006 [Chen] ¶ 382), is the process of using “motion compensation” to predict where the next bits will be. When video is encoded/compressed, the smaller frames such as B and P, already use this information for compression purposes. By predicting where bits will be, not all bits have to be encoded into the encoded stream. In Temporal Scalability coding, extra information is baked into each frame to enhance this. Thus, entire frames can be lost without significant drops in quality because they can be predicted or mostly predicted. Obviously, partial encryption is useless without these components because the “predictive” information from unencrypted portion of a layer may be used to reconstruct the information in an encrypted portion of another layer.

Ex. 2012 [Nielson Decl.] ¶ 66.

A similar problem—unencrypted portions being used to decrypt encrypted portions—exists with attempting to implement partial frame encryption in connection with the FEC feature of Chen.

As explained above, FEC provides correction information for packets in advance of the packets actually being received. If each packet is only partially encrypted, then the information from an unencrypted portion of an earlier packet may be used to decrypt the encrypted portion of a later packet without the need for the encryption key. For example, if packets 1-7 include FEC bits that allow for the reconstruction of packets

8-10, then the unencrypted portions of packets 1-7 could be used to determine the information contained in the encrypted portion of packets 8-10. This is a similar problem to the one I explained in connection with independent scalable layers.

Ex. 2012 [Nielson Decl.] ¶ 68.

Moreover, even if the issue of compromising encryption was overcome in connection with FEC, there are additional aspects of Chen's FEC that would need to be resolved if implemented with partial encryption:

Chen utilizes FEC to reconstruct packets that have not arrived yet. In other words, earlier arrived packets will be used to reconstruct packets that have not arrived yet, without the need to actually receive those packets. Yet, Chen would not be able to actually reconstruct the not-yet-arrived packets unless it also has the encryption information, such as what portion of a frame is encrypted, in advance. Thus, unless Chen also obtains, *in advance of actually receiving the packet* that is lost in transmission, encryption parameters that identify the portions of the lost packet that are encrypted, Chen would not be able to utilize the FEC information for the lost packet. In other words, reconstructing an encrypted packet through the use of FEC data, but not being able to decrypt that reconstructed packet because the client has not yet received the encryption parameters for that packet, would render FEC useless.

Ex. 2012 [Nielson Decl.] ¶ 69 (emphasis in original).

As Dr. Nielson explains, even if these hurdles are surmountable, "they are far beyond the level of skill of a POSITA":

Dr. McDaniel testifies that a POSITA has only one or two years of experience in “video streaming and media security.” Ex. 1003, ¶ 67. I do not believe that a person with this level of experience could implement partial frame encryption in the context of Chen’s system. As explained above, Chen’s layers could easily compromise the encrypted portions in a partially encrypted frame because unencrypted portions of a parallel layer could be used to fill-in encrypted portions. Similarly, Chen’s use of FEC could cause a similar problem of unencrypted portions revealing encrypted portions. Even if this issue could be overcome, there are also other additional challenges such as timing and manner of transmission of encryption parameters for packets that have not yet arrived, but are reconstructed using FEC. These are each significant hurdles that Petitioner and Dr. McDaniel do not address. I believe each of these problems is far beyond the level of skill of a POSITA because, *inter alia*, they involve complex mathematical, technical and system design aspects that well exceed the knowledge and experience of a POSITA.

Ex. 2012 [Nielson Decl.] ¶ 70.

The challenges of *ex post facto* integrating partial frame encryption into Chen’s system is hardly surprising as leading experts in cryptography understand that, “[y]ou can’t make systems secure by tacking on cryptography as an afterthought” and that, rather, “[y]ou have to know what you are doing every step of the way, from conception through installation.” Ex. 2018 [Schneier] 1; Ex. 2017 [Schnier Blog] 1. As Dr. Nielson explains:

It is also well known that there is a great difference between those that *create* cryptographic systems and those that *use* them. The entire purpose of the *Crypto Done Right* project, which I co-founded, is to better help the users of cryptography know the proper configurations and deployments of these systems. The creators of cryptography typically understand the implications of different configurations and different deployments, but this information is often not transferred well to those that use these systems. In my opinion, the POSITA described by Dr. McDaniel is, at best, a user of cryptography. If it is possible to combine partial encryption and FEC/scalable encoding, it will be necessary to employ a person with deeper understanding of creating cryptographic systems, who would be an expert in the field, not a mere POSITA.

Ex. 2012 [Nielson Decl.] ¶ 71 (emphasis in original).

Therefore, Petitioner fail to prove that a POSITA would not have a reasonable expectation of success in implementing partial frame encryption in Chen's system which also utilizes FEC and independent scalable layers.

3. A POSITA Would Not Have Been Motivated To Combine Chen And Lindahl Without Chen's Integral Features Because That Would Reduce, Not Improve, Efficiency.

The Petition's proffered motivation to combine Lindahl's partial frame encryption in Chen is to "address piracy concerns and improve efficiency." Pet., 18. However, as will be discussed in this section, modifying Chen to implement partial frame encryption is neither needed "to address piracy concerns," nor does it

“improve efficiency.” Rather, Petitioner’s combination would undermine security and deteriorate Chen’s “efficiency” by destroying integral aspects of Chen that are used to improve its latency, user experience and efficiency.

Petitioner’s first proffered motivation of implementing “partial frame encryption” in Chen to “address piracy concerns” is misplaced. Chen already discloses fragment level encryption which addresses piracy concerns. Petitioner makes no showing whatsoever that Lindahl’s system, which only partially encrypts a frame, provides better protection or that Chen’s own fragment level encryption does not provide sufficient “piracy” protection. Rather, and as discussed in the preceding section, implementing partial frame encryption in Chen’s system (assuming such a thing could be done) would likely undermine security in view of Chen’s scalable layers and FEC method, both of which could allow unencrypted portions decrypt encrypted portions when combined with partial frame encryption. *See also* Ex. 2012 [Nielson Decl.] ¶ 72.

Nor does Petitioner’s unsupported assertion that implementing Lindahl would “improve efficiency” hold water. As discussed in the immediately preceding sections, a POSITA would not have had a reasonable expectation of success in devising a partial encryption method for a system, such as Chen, that utilizes both independent scalable layers and FEC. Moreover, eliminating those features of Chen would substantially deteriorate Chen’s performance and reduce its efficiency. For

example, Chen discloses that its independent, scalable layers are central to an acceptable user experience. Chen explains that in the absence of its independent, scalable layers, user stalls can still be avoided but at the cost of substantially reduced user experience:

Stalls can be avoided, reduced or mitigated by restricting a data rate of the representations chosen to be much less than the available bandwidth, so that it becomes very unlikely that any given portion of the presentation would not be received in time, but this strategy has the disadvantage that the media quality is necessarily *much lower* than could in principle be supported by the available bandwidth. A lower quality presentation than is possible also can be interpreted as *a poor user experience*.

Ex. 1006 [Chen] ¶ 379; *see also* Ex. 2012 [Nielson Decl.] ¶¶ 73-74. Again, the Petition provides no analysis, argument, or even acknowledgement of why a POSITA would have been motivated to create “a poor user experience” just to implement partial frame encryption.

Similarly, in connection with its use of FEC, Chen explains that “[t]he advantages of cooperative HTTP/TP requests together with usage of FEC repair data may be especially important to provide consistently quick channel zapping times.” Ex. 1006 [Chen] ¶ 528. Chen then conducts an analysis of its system’s performance with and without FEC, *id.*, ¶¶ 529-533, and finds that by implementing FEC, it improved performance by up to 70%. *Id.*, ¶ 533 (“Thus, in the example shown in

Fig. 26, the No-FEC method is 70% worse in terms of channel zapping time than the FEC method.”); *see also id.*, Figs. 24-26; Ex. 2012 [Nielson Decl.] ¶ 75. The Petition provides no analysis, argument or even acknowledgement of why a POSITA would have been motivated to reduce Chen’s timing performance just to implement partial frame encryption.

The absence of any motivation to implement partial frame encryption in Chen is also supported by the fact that, as Dr. Nielson explains, there were other methods of reducing the encryption burden on the system which were compatible with Chen, but that did not include partial frame encryption:

even if a POSITA desired to reduce the encryption burden in Chen, he or she would have likely implemented the much more routine and much simpler process of encrypting some, but not all, fragments, on a periodic basis. For example, a POSITA could have encrypted, *e.g.*, every other fragment. Interestingly, the Petition argues that a POSITA “would have found it obvious to partially encrypt *all* frames,” Pet., 30, yet, it is not apparent why such partial frame encryption has any advantage to “improve efficiency” over encrypting, for example, every other fragment—especially in light of Chen’s incompatibility with partial frame encryption. Notably, encrypting some, but not all, fragments in Chen does not create the same problems identified in connection with partial frame encryption because Chen’s FEC and scalability layers are performed within individual fragments. Thus, an unencrypted fragment cannot be used to reconstruct another encrypted fragment.

Ex. 2012 [Nielson Decl.] ¶ 76; *see also id.*, ¶ 67; Ex. 2013 [McDaniel Depo.] 110:22-111:5; 113:407.

It was Petitioner’s burden “to explain how and why” the disparate features of Chen and Lindahl would have been combined to arrive at the claimed invention. *Samsung Elecs. Co. Ltd. v. Kaist IP US LLC*, IPR2017-01046, Paper 14 at 7 (PTAB, Jan. 22, 2018). Merely identifying elements in the prior art is not sufficient to establish obviousness. Petitioner here has failed to meet its burden to show why a POSITA would have been motivated to attempt implementing partial frame encryption in Chen at the cost of removing its integral features that, for example, improve its timing by 70%. *Hulu LLC v. Sound View Innovations LLC*, IPR2018-00582, Paper 34 at 20-21 (PTAB Aug. 5, 2019) (informative) (rejecting Petitioner’s proposed combination because Petitioner had not “adequately supported” why it would have been “good idea” to modify references as proposed).

Thus, the Petition fails due to this deficiency, which affects Petitioner’s arguments with respect to all claims.

4. The Need To Modify Standard File Formats Would Further Counsel A POSITA Against Combining Chen And Lindahl.

A POSITA would additionally not have been motivated to implement a partial frame encryption in Chen because that would require a POSITA to make substantial changes to the standard file formats utilized by Chen—a task that the Petition does not even attempt to show was within the skills of a POSITA. *Hulu LLC v. Sound*

View Innovations LLC, IPR2018-00582, Paper 34, 19 (PTAB Aug. 5, 2019) (informative) (noting “other disadvantages” of the proposed combination in rejecting Petitioner’s arguments).

It is undisputed that to even attempt implementing partial frame encryption in Chen, it was required to implement modifications to the standard file formats utilized by Chen—a challenging task in and of itself:

Q. Do any of the embodiments that you rely on from Chen in your declaration require a modification of a standard file format in order to enable encryption?

A. Yeah, I think the combination—we are talking about Chen with, you know, using things like partial encryption would require some additional encryption information. For example, to process the contents, so you would probably have to make some modifications to 3GPP to enable or to—not enable—to implement the combination of Chen, Hurst and Lindahl.

Ex. 2013 [McDaniel Depo.] 35:25-36:12; *see also* Ex. 2013 [McDaniel Depo.] 25:7-18; 34:11-14 (testifying that the neither the Matroska nor the MP4 and nor the 3GPP standard file formats permitted inclusion of the DRM information within the file as disclosed by the ’588).

Notably, Dr. McDaniel does not opine that a POSITA would have been able to modify any of the standard file formats. Rather, Dr. McDaniel opines that the level of ordinary skill was to merely “*us[e]* known video container file formats for

streaming, such as the ISO base media file format, sometimes referred to as the MP4 container format, and 3GPP extensions to the ISO base media file format.” Ex. 1003 [McDaniel Decl.] ¶ 68. Instead, it was beyond the skills of a POSITA to modify the standard file formats to implement partial frame encryption information within the file. Ex. 2012 [Nielson Decl.] ¶¶ 78-82, 71.

In contrast, as discussed in section III.A, *infra*, the ’588 Patent enables this combination by disclosing, at length, how to modify the Matroska standard file format so that encryption information and parameters to partially encrypt frames can be efficiently included in the file and in the requested portion of the stream.

Therefore, this is yet another reason why Petitioner has failed to show that a POSITA would have a motivation, or even a reasonable expectation of success, to combine Chen and Lindahl.

III. PETITIONER FAILS TO SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS “LOCATING ENCRYPTION INFORMATION...WITHIN THE REQUESTED PORTIONS OF THE SELECTED STREAM OF PROTECTED VIDEO” (ALL CLAIMS).

Challenged independent claims 1 and 12, each require, *inter alia*:

Locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video.

Ex. 1001 [’588 Patent] cls. 1, 12. The “selected stream” refers to the claims’ requirement that one of a “plurality of alternative streams of protected video” is

“select[ed].” The remaining challenged claims depend from either claim 1 or claim 12. Petitioner fails to prove that any of the claims are unpatentable as it fails to demonstrate that this limitation, properly construed, is obvious over the proffered combination.

The Board has preliminarily construed this limitation such that “within the requested portions of the selected stream of protected video” modifies “portions of frames of video.” Inst. Dec., 28-31. In other words, the recited “encryption information” can be “located” anywhere under the Board’s preliminary construction. *Id.* As discussed in detail in Section III.A., *infra*, Patent Owner respectfully disagrees with the Board’s provisional construction. The claim language, in view of the specification, makes clear that the limitation “within the requested portions of the selected stream of protected video” modifies “locating,” and requires that the “encryption information” be “located” “within the requested portions of the selected stream of protected video.”

The Petition relies solely on Lindahl for the disclosure of the “locating” step. Pet., 52-55. However, to the extent that Lindahl locates any encryption information, it does not locate the information “within the *requested portions* of the *selected stream* of protected video,” as the claims, properly construed, require. In fact, Lindahl cannot teach this limitation, because it does not relate to a system in which content is partially requested or one of a plurality of “alternative streams” is

“selected.” *See* Section III.B, *infra*. The Petition also offers no basis to modify Lindahl to disclose this limitation. *See* Section III.C, *infra*.

A. The Plain Meaning Of The Claims And Every Embodiment In The ’588’s Specification Requires “Locating Encryption Information” “Within The Requested Portions Of The Selected Stream Of Protected Video.”

Both the plain meaning of the claims and the ’588’s specification confirm that the clause “within the requested portions of the selected stream of protected video” in the “locating” step of the challenged claims modifies “locating encryption information,” and, properly construed, dictates that the “encryption information” must be “located,” “within the requested portions of the selected stream of protected video.” Ex. 2012 [Nielson Decl.] ¶ 85.

Claim construction begins with the language of the claims. *Northern Telecom Ltd. v. Samsung Elecs. Co.*, 215 F.3d 1281, 1287 (Fed. Cir. 2000). The language of the limitation-in-question, states:

[1] ***Locating encryption information*** [2] that identifies encrypted portions of frames of video [3] ***within*** the requested portions of the selected stream of protected video

’588, cl. 1. As Dr. Nielson explains, a POSITA would understand that the most natural reading of the claim is that the “within” clause modifies the “locating” clause:

A POSITA would understand that the first clause of the limitation requires “**locating** encryption information.” The next clause—“**that** identifies encrypted portions of frames of video”—informs a POSITA regarding the function of the “encrypted information.” The last clause—“**within** the requested portions of the selected stream of protected video”—informs a POSITA where the “**locat[ed]** encrypted information” is “located.” Therefore, a POSITA would interpret the limitation as requiring the “encryption information” to be “located” “within the requested portions of the selected stream of protected video.”

Ex. 2012 [Nielson Decl.] ¶ 87; *see also id.*, 85-86. In accord with Dr. Nielson’s testimony, there is, of course, a natural relationship between the verb “locating” and “within” such that “within” refers to where the encryption information is “located.” Thus, the most natural reading of the limitations indicates that the encryption information is “located” “within the requested portions of the selected stream of protected video.”

This natural reading of the claim limitation accords with and is reinforced by every embodiment in the ’588’s specification. *See Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1319 (Fed. Cir. 2005) (“We cannot look at the ordinary meaning of the term . . . in a vacuum. Rather, we must look at the ordinary meaning in the context of the written description and the prosecution history.”) (citation omitted). In particular, it is undisputed by the experts that in **every embodiment** of

the '588, “encryption information” is located within the “requested portion” of the video. Ex. 1001 ['588 Patent] 9:23-29; 13:57-63; 16:33-49; 22:14-17; 25:10-21; Ex. 2013 [McDaniel Depo.] 47:2-49:20; 55:5-15 (confirming encryption information located within requested portion of stream within each of the '588's embodiments); Ex. 2012 [Nielson Decl.] ¶ 88.

For instance, in one embodiment, the specification explains that once the requested portion of the video (referred to as a “BlockGroup”) is received, it is “parsed” for the DRMInfo (*i.e.*, “encryption information”) that identifies the encrypted portions of the frame (*i.e.*, “locating the encryption information within the requested portions of the video”):

[E]ach of the Matroska container files containing an alternative stream of protected video includes *a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted* ..., and the client application configures the processor to access video frames in a stream of protected video using the common cryptographic information by configuring the processor to: obtain a BlockGroup containing a protected frame of video; *parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted* using an encryption key from the set of encryption keys ...

Ex. 1001 ['588 Patent] 4:39-58. Thus, this embodiment teaches “locating” the encryption information (“DRMInfo”) in the “requested portion” (“BlockGroup”) as

the “BlockGroup element” is “parse[d]” “to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted ...” Ex. 2012 [Nielson Decl.] ¶ 89.

Indeed, locating encryption information within the requested portions of the stream is one of the central aspects of the ’588’s inventive system. Ex. 2012 [Nielson Decl.] ¶ 90. This is evidenced by the fact that the inventors did not simply utilize the industry standard Matroska container file, but, rather, modified the Matroska file format to add this aspect of the invention:

In many embodiments, *the Matroska container files are specialized Matroska container files that include enhancements (i.e., elements that do not form part of the Matroska file format specification)* that facilitate retrieval and decryption using common cryptographic information of specific portions of media during adaptive bitrate streaming.

Ex. 1001 [’588 Patent] 11:45-50. The modified Matroska container file is schematically shown in Patent’s Fig. 4e, reproduced below. As can be seen, the “DRM Info” (*i.e.*, encryption information) highlighted in yellow is located within each BlockGroup (*i.e.*, a “requested portion of the video,” ’588, 16:21-52):

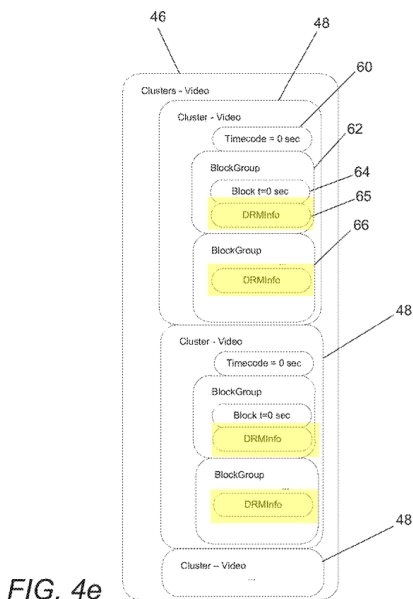


FIG. 4e

'588, Fig. 4e; *see also* Ex. 2013 [McDaniel Depo.] 25:7-18; 34:11-14 (testifying that the neither the Matroska nor the MP4 and nor the 3GPP standard file formats permitted inclusion of the DRM information within the file as disclosed by the '588); Ex. 2012 [Nielson Decl.] ¶ 90.

Thus, the '588's specification of the Patent, including every embodiment therein, supports Patent Owner's construction. *Kinetic Concepts, Inc. v. Blue Sky Med. Grp., Inc.*, 554 F.3d 1010, 1018-19 (Fed. Cir. 2009) (limiting "wound" to "skin wounds" where "[a]ll of the examples described in the specification involve skin wounds"); *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1149-50 (Fed. Cir. 2012) (construing "electrochemical sensor" to exclude external cables or wires where "every embodiment shows an electrochemical sensor without external cables or wires"); *Wisconsin Alumni Res. Found. v. Apple Inc.*, 905 F.3d 1341, 1351-52 (Fed.

Cir. 2018) (limiting “prediction” to dynamic prediction where all embodiments describe dynamic prediction and allowing the term to cover static prediction “would ‘expand the scope of the claims far beyond anything described in the specification’”); *Choon's Design, LLC v. IdeaVillage Prods. Corp.*, 776 Fed App'x 691, 695-96 (Fed. Cir. 2019) (construing “at least one pin bar” to extend only to detachable pin bars, where “the specification discloses only loom kits having detachable bases and pin bars”).

In making its preliminary claim construction to the contrary, the Board quotes the '588 patent at 24:63-25:2 for the proposition that the encryption information can be located anywhere and does not have to be located within the requested portions of the stream. Inst. Dec., 29-30. However, as Dr. Nielson explains:

[The '588 at 24:63-25:2] relates to an index of byte ranges of the streaming media that would allow the client to select which byte ranges of the streaming media to request for viewing. This sentence does not relate to the location of **encryption information** that identifies which portions of the frames within those requested byte ranges are encrypted. As discussed above, once the selected portions of video are actually received by the client, the encryption information is located within those selected portions. Thus, the specification does not support the Board's preliminary construction.

Ex. 2012 [Nielson Decl.] ¶ 91; *see also id.*, ¶ 84.

The Board's preliminary construction also relied upon a grammatical treatise's guidance on best practices:

A common treatise on grammar teaches that “[t]he position of words in a sentence is the principle means for showing their relationship,” and “[t]he writer must, therefore, bring together the words and groups of words that are related in thought and keep apart those that are not so related.” William Strunk, Jr. & E.B. White, *The Elements of Style* 36 (4th ed. 2000).

Inst. Dec., 30.

But the limitation-in-question as properly understood is also consistent with other examples from the very same treatise. Strunk & White provide as an exemplary sentence: “[t]he lawn mower that is broken is in the garage.” Ex. 2014 [Strunk & White] 87. This sentence indicates that the lawn mower is (a) broken and (b) in the garage. Another noted treatise on style, Bryan Garner's *The Redbook, A Manual on Legal Style*, provides a similar example: “The meeting that starts at 10 a.m. is about the Matthews case.” Ex. 2015 [Garner] 5. Here too, the meeting (a) starts at 10 a.m. and (b) is about the Matthews case. The limitation-in-question has the same structure as these examples. It says “locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video.” The “located encryption information” (a)

identifies encrypted portions of frames of video and (b) is within the requested portions of the selected stream of protected video.

Additionally, the best practice that Strunk & White identifies is inapplicable here because the second and third clauses of the limitation ***both*** modify the first clause and they cannot both follow immediately after the first. The limitation certainly would not be clearer if the limitation were written such that the third clause followed the first:

[1] ***Locating encryption information*** [3] ***within*** the requested portions of the selected stream of protected video [2] that identifies encrypted portions of frames of video

Further, it is well-settled that it is the actual words of the limitation that are of primary importance in claim construction. The limitation again requires “***locating*** encryption information,” the next clause tells us what the “encryption information,” does and the third clause tells us where the “encryption information” to be “locat[ed]” is located. This natural reading, again, is consistent with every embodiment in the ’588, as Dr. McDaniel conceded in deposition. Ex. 2013 [McDaniel Depo.] 47:2-49:20; 55:5-15. As Dr. Nielson also explains, “I do not believe that the grammatical preference identified by the Board would alter a POSITA’s understanding of the limitation, especially in light of the ’588’s specification discussed above.” Ex. 2012 [Nielson Decl.] ¶ 92.

Moreover, generalized, non-specific grammatical best practices, shorn of context, are not sufficient to dictate a claim construction, especially in light of the '588's specification that expressly counsels in favor of Patent Owner's construction. *Kingsley v. United States*, 24 Ct. Cl. 219, 222-223 (1889 Ct. Cl.) ("The language of the section, grammatically considered, might justify that construction, but other considerations indicate that Congress did not so intend it."); *Nestle's Food Co. v. United States*, 16 Ct. Cust. 451, 455 (1929 Ct. Cust. App.) ("While it is the general rule that a dependent or modifying clause relates to and modifies its nearest antecedent, such rule must yield, if to adhere to it would defeat the purpose of the Congress."). Applying the above principle, the Federal Circuit recently reversed a district court claim construction in *Quality Edge, Inc. v. Rollex Corp.*, 709 Fed. Appx. 1000, 1006 (Fed. Cir. 2017). Noting that there was no "hard and fast" grammatical rule, the specification of the patent there mandated an alternative construction to the one suggested by a general grammatical best practice. *Id.*, 1007.

For the foregoing reasons, the "locating" limitation, properly construed, requires, *inter alia*, that "encryption information" be "locat[ed]" "within the requested portions of the selected stream of protected video." This construction is consistent with both the plain meaning of the claim and every embodiment in the '588.

B. Petitioner Fails To Prove That The Lindahl/Chen Combination Teaches Or Renders Obvious Locating Encryption Information Within Requested Portions Of The Selected Stream As Claimed.

As discussed above, the “locating” limitation of claims 1 and 12 requires, *inter alia*, “locating encryption information” “within the requested portions of the selected stream of protected video.” The Petition contends that this limitation is disclosed exclusively by Lindahl and does not rely upon Chen or Hurst for any modification of Lindahl. Pet., 52-54. Specifically, Petitioner contends that Lindahl’s variables X, Y, and Z teach the claimed “encryption information.” Pet., 54.

But, even if variables X, Y, and Z were such “encryption information,” there is no possibility of Lindahl teaching locating said information “within the requested portions of the selected stream of protected video” as claimed. Lindahl is not a streaming system in which “portions” of a “selected stream,” amongst a “plurality of alternative streams” is “requested.” Rather, Lindahl is system in which the entire media, which is contained in a file, is downloaded for later play back. Additionally, Lindahl only permits transfer and decryption of media once the entire media file has been downloaded. Ex. 1007 [Lindahl] ¶ 66 (“Once the media file is downloaded 708, the media file can then be decrypted 710 at the user’s local machine using the cryptographic key.”); *see also* Ex. 2012 [Nielson Decl.] ¶¶ 95-96. Petitioner’s expert admitted at deposition that there is no embodiment of Lindahl where a user can request only parts of a media file:

Q. Is there any embodiment of Lindahl where the user can request only parts of a media file?

A. So I don't see one as I am looking here

Ex. 2013 [McDaniel Depo.] 69:18-20.

Thus, the concepts of “portions” of a video and “alternative streams” simply do not exist in Lindahl. Ex. 2012 [Nielson Decl.] ¶ 97. Regardless of whether Lindahl locates any encryption information, it cannot locate any encryption information within the “requested portions” of the video because a user in Lindahl can never request a portion of a video, much less one from a “selected stream.” Therefore, even if Lindahl is combined with Chen, and even if Chen does request portions of a video, there is nothing in the record to disclose locating encryption information “within the requested portions of the selected stream,” as opposed to some other location. The Petition does not address why a POSITA would modify Lindahl, Chen or the combination of Lindahl/Chen to locate the encryption information within the requested portions of video. As discussed in Section III.A, *supra*, the '588 specifically teaches modifying a standard file format in order to be able to locate the encryption information “within the requested portion of video”—a feature absent in all of Petitioner’s references.

Thus, Lindahl simply cannot disclose the claim limitation, present in all challenged claims, of “locating encryption information ... within the requested portions of the selected stream of protected video.”

C. Petitioner Offers No Basis To Modify Lindahl To Disclose “Locating Encryption Information Within The Requested Portions Of The Selected Stream Of Protected Video.”

The Petition does not argue that it would be obvious to modify Lindahl to disclose “encryption information” within “requested portions” of a selected stream. Rather, the Petition merely asserts that:

It would have been obvious to retrieve the encryption parameters to identify the encrypted portions of the content so that they may be decrypted efficiently.

Pet., 55. But this allegation of “obviousness,” even if true, does not relate to *where* the encryption information is located, let alone being located “within the requested portion” of the “selected stream” as the properly construed claims require. The Petition simply does not suggest any modification to Lindahl (or other aspects of its combination) that would practice the limitation. *See, e.g., Microsoft Corp. v. IpLearn-Focus LLC*, IPR2015-00095, Paper 33, 29 (PTAB Apr. 11, 2016) (rejecting obviousness argument because “Petitioner has not presented an analysis sufficient to support modifying [the single reference] beyond the teachings of [the reference] itself.”); *see also Hulu LLC v. Sound View Innovations LLC*, IPR2018-00582, Paper 34, 20-21 (PTAB Aug. 5, 2019) (informative) (rejecting Petitioner’s proposed

combination because Petitioner had not “adequately supported” why it would have been “good idea” to modify references as proposed).⁴

For all these reasons, the Petition fails to meet its burden to prove by a preponderance of the evidence that its combination renders the “locating” limitation obvious.

IV. PETITIONER FAILS TO SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS VIDEO FRAMES IN ALTERNATIVE STREAMS “THAT ARE ENCRYPTED USING A SET OF COMMON KEYS” (ALL CLAIMS).

The Petition’s sole Ground fails for another reason. Each of the challenged claims requires that video frames of the alternative streams of the protected content be “encrypted using a set of common keys comprising at least one key.” Ex. 1001 [’588 Patent] cls. 1, 12. The Petition fails to demonstrate that Chen in view of

⁴ Dr. McDaniel’s declaration also does not bridge the gap in the Petition’s analysis. To the extent that it provides any additional arguments, however, as insufficient as they may be, they should not be considered by the Board as they are not developed in the Petition. *See, e.g., Cisco Sys., Inc. v. C-Cation Techs., LLC*, IPR2014-00454, Paper 12, 9-10 (PTAB Aug. 29, 2014) (informative) (“we will not consider arguments that are not made in the Petition, but instead are incorporated by reference to the cited paragraphs...of [an expert] Declaration” “to support conclusory statements that are not otherwise supported in the Petition”).

Lindhahl and Hurst renders this limitation obvious. The Petition relies only on its secondary references for the limitation requiring “a set of common keys,” arguing that “Lindhahl and Hurst both teach or suggests [*sic*] this limitation, and either is sufficient by itself to render the limitation obvious.” Pet., 30-35. Petitioner’s argument should be rejected for the reasons that follow.

A. The Petition Fails To Show That Chen In View Of Lindahl Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.

Petitioner first relies on Lindahl for the disclosure of encrypting video frames in alternative streams of content using “a set of common keys.” Pet., 31-32. Lindahl, however, does not address the situation of encrypting video frames in a plurality of alternative streams of content, whether using the a “set of common keys” or otherwise. *See* Section IV.A.1, *infra*. To the extent that Lindahl does provide any relevant disclosure, it teaches *against* utilizing a set of common keys for different media files, and only uses a “global key” for unimportant metadata associated with the files. *See* Section IV.A.2, *infra*. The Petition fails to show why a POSITA would have been motivated to modify Chen in view of Lindahl to disclose this limitation. *See* Section IV.A.3, *infra*.

1. Lindhahl Does Not Disclose A Streaming System With Alternate Streams Of The Same Content.

The limitation-in-question again requires that “each of the alternative streams of protected video includes partially encrypted video frames that are encrypted using

a set of common keys comprising at least one key.” As discussed in this section, Lindahl cannot disclose this limitation because it simply does not disclose “alternative” streams of a given video, much less what keys to use for them. As discussed in the following sections, Petitioner’s arguments to the contrary are misplaced.

Lindahl has nothing to do with “alternative streams of protected video.” Lindahl is not even about streaming media, let alone streaming media with alternative streams of the same content. Lindahl utilizes a system that downloads an entire media, which is contained in a file, onto the user device, which can then access the content at any time for playback. Ex. 1007 [Lindahl] ¶¶ 40, 66, 68; *see also* Ex. 2012 [Nielson Decl.] ¶¶ 95-96, 100-101. Petitioner’s expert was also forced to admit at his deposition that Lindahl does not disclose streaming media with alternative streams of the same content:

Q. Is there any embodiment in Lindahl that discloses multiple alternative bitrates encoding of media file?

A. Again, *that’s not the purpose of Lindahl*, you know.

Ex. 2013 [McDaniel Depo.] 70:6-10; 71:12-16; *see also* 69:15-16 (“Lindahl does not have a direct embodiment that has streaming data in it.”).

Lindahl’s system, wherein an entire media file is downloaded at one time and played back later, lies in sharp contrast to the real-time streaming challenges

addressed by the '588. The '588 discloses that adaptive bitrate streaming, where the user selects and switches between various alternative streams encoded at different bitrates, is a situation that arises in the context of real-time streaming media, because of fluctuations in network conditions that may affect user experience:

Adaptive bit rate streaming or adaptive streaming involves detecting the present streaming conditions (e.g., the user's network bandwidth and CPU capacity) *in real time and adjusting the quality of the streamed media accordingly* by selecting between different streams encoded for use at different network connection data rates. Typically, the source media is encoded at multiple bitrates and the playback device or client switches between streaming the different encodings depending on available resources.

Ex. 1001 ['588 Patent] 1:59-67. By contrast, and as Hurst confirms, systems like Lindahl's wherein "[m]edia files [are] prepared for downloading and storing usually are encoded with a higher quality audio/video than can be delivered in real time."

Ex. 1008 [Hurst] 1:31-38; *see also* Ex. 2012 [Nielson Decl.] ¶ 102.

Lindahl's system references "streaming" twice, but both disclosures are immaterial. In the first instance of use of the word "stream media," Lindahl mentions that "[t]he remote media source 106 can transmit or stream media files to the media server 102." Ex. 1007 [Lindahl] ¶ 39. That reference to "stream[ing]" is neither real-time nor adaptive streaming, in which media is continuously sent over the network and consumed by the user in real time, which is the kind of streaming

of media that would benefit from alternative streams. *See* Ex. 1001 [’588 Patent] 1:45-49; Ex. 1006 [Chen] ¶ 21. Instead, this reference in Lindahl to stream is merely a synonym for “transferring,” referring to transferring the file from the content provider to the server, not to the user. Ex. 1007 [Lindahl] ¶ 39 (“The media files that are received at the media server 102 from the media sources 104, 106 can be processed ***and then stored*** to a media storage 110.”). This is undisputed. Ex. 2013 [McDaniel Depo.] 66:4-9. In that context, the word “stream” is used in the sense of transmitting files to a server for storage and later download. Ex. 2012 [Nielson Decl.] ¶ 103. Transfer of files to a backend server does not even present the occasion for alternative bitrate streaming. *Id.*

In the second instance of the use of the word “streaming,” Lindahl mentions that “the download 708 of the media file can be performed by streaming the media file through the data network to the user, namely, to the user’s client machine.” Ex. 1007 [Lindahl] ¶ 65. Again, this reference is also only merely referring to the transfer of the file, not real time streaming or adaptive bitrate streaming. This is confirmed by the fact that in the immediately following step, Lindahl explains that the file cannot be decrypted until “the media file is downloaded.” *Id.*, ¶ 66. If it cannot be decrypted until it is completely downloaded, it follows that it cannot be streamed in real-time such that alternative streams might be present. Ex. 2012 [Nielson Decl.] ¶ 104. Petitioner’s expert admitted to the same at his deposition:

Q. Is it your contention that reference to streaming in Paragraph 65 of Lindahl, is referencing streaming media and the fact that the user consumes the media as it is received and before the entire file is downloaded?

A. No.

Ex. 2014 [McDaniel Depo.] 65:4-9.

Thus, because Lindahl addresses a system where files are downloaded, as opposed to adaptively streamed for real-time playback, Lindahl does not address any situation where alternative streams of the same video content are presented for selection by the user, as occurs in the streaming to which the '588 Patent and this particular limitation is directed. Such alternative streams do not exist in Lindahl's system. Therefore, Lindahl simply has no teaching regarding what keys to use for alternative streams of the same video.

2. Lindahl Teaches Using A Global Key To Encrypt Some Metadata, Not Content.

Despite the fact that it is undisputed that Lindahl does not even disclose a system with alternative streams of video, the Petition argues that Lindahl nevertheless teaches encrypting alternative streams of protected video using a “set of common keys,” because Lindahl teaches the use of a global key, which the Petition argues discloses the claimed “set of common keys.” Pet., 30-32. Its

argument falls flat at least because Lindahl never uses a global key to encrypt video frames, as the claims require, but only metadata.

First, the Petition contends that “*Lindahl* teaches or suggests that media files may be encrypted...with a global key.” Pet., 31. But Lindahl never discloses that *media files* may be encrypted with a global key. Rather, Lindahl only teaches that *metadata* associated with a media file, but *not* the media data within the file, may be encrypted with a global key—and even for metadata, Lindahl teaches the use of global key only for certain metadata that “is not that sensitive” so that “stronger encryption” is not needed:

The media file is construed such that it includes media data and may further include metadata. The metadata describes characteristics of the data. For example, metadata can indicate characteristics, such as name, artist, copyright information, title, etc. The metadata of the media file is optionally encrypted, such as with a global key. In one embodiment, the *global key is used to encrypt the metadata* for all the media files at the media server. In another embodiment, if desired, different global keys can be used with different media servers. *Typically, the metadata is not that sensitive so the use of a common global key to encrypt such is adequate.* However, *if stronger encryption is desired, then more specialized keys can be used to increase the level of security.*

Ex. 1007 [Lindahl] ¶ 48. The Patent’s claim limitation, however, does not address encryption of metadata. Rather, the claims expressly require encryption of video frames of the alternative streams using a set of common keys—just the sort of more

sensitive content that Lindahl teaches needs “stronger encryption” than a global key. *See* Ex. 1001 [’588 Patent] cl. 1, 23:43-53; Ex. 1007 [Lindahl] ¶ 48; *see also* Ex. 2012 [Nielson Decl.] ¶¶ 106-108.

The Petition relies on the following section of Lindahl to argue that Lindahl discloses encrypting all files within a server, and thus alternate streams of the same video, with a single global key:

Once the media file is downloaded 708, the media file can then be ***decrypted*** 710 at the user’s local machine using the cryptographic key. The global key or other cryptographic key may also be used. If the metadata of the media file itself is encrypted, the metadata can also be decrypted using the global key which has previously been provided to the user who has purchased the access rights to the media file.

Ex. 1007 [Lindahl] ¶ 66; *see also* Ex. 2013 [McDaniel Depo.] 79:14-18 (“Q. [O]ther than Paragraph 66, there are no other disclosures in Lindahl that [you] contend discloses encrypting a video frame with a global key? A. I don’t see any, as I am sitting here right now.”).

The cited section of Lindahl, however, never discusses encryption with a global key. It only references “decryption.” There is no mention of encryption of an entire file (as opposed to just the metadata) with a global key anywhere in Lindahl. So, at best, this section of Lindahl that mentions decryption with a global

key with no corresponding disclosure of encrypting with a global key is ambiguous. Ex. 2012 [Nielson Decl.] ¶¶ 109-110.

The Petition attempts to explain this ambiguity by importing a non-existent disclosure into Lindahl, arguing that Lindahl necessarily uses a symmetric key system and therefore there must be an encryption of all files with a global key inherent in Lindahl. Pet., 31, citing Ex. 1007 [Lindahl] ¶ 8. As a preliminary matter, the portion of Lindahl cited by Pet. 31 discusses general background on encryption regarding the existence of both symmetric and asymmetric encryption. Ex. 1007 [Lindahl] ¶ 8. It is silent on what type of encryption paradigm Lindahl may—let alone must—use.

The simpler explanation, however, is that Lindahl's reference to decryption with a global key does in fact correspond to a disclosure within Lindahl for encryption with a global key—as would be normally expected since encryption and decryption both have to happen, and not necessarily with the same key. That means that the reference to decryption with a global key in Lindahl ¶ 66 in fact corresponds to the only reference in Lindahl for encryption with a global key at Lindahl ¶ 48. As previously discussed, Lindahl ¶ 48 discloses using a global key only for metadata associated with a file, and never for actual video frames, as the claim requires. In fact, to interpret Lindahl to disclose using a global key for every file in a server would conflict with Lindahl's careful discussion in ¶ 48, where it explained that

only unimportant metadata should be encrypted with a global key. Ex. 2012 [Nielson Decl.] ¶ 111.

Therefore, Lindahl fails to teach using a global key to encrypt alternate streams of video—as opposed to using the global key for just metadata.

3. It Would Not Have Been Obvious To Modify Chen In View Of Lindahl To Encrypt Alternate Streams Of Protected Video With A Global Key.

The Petition next argues that Lindahl’s disclosure of encrypting just metadata within a file with a global key renders it obvious to modify its teachings to instead encrypt “alternative streams” of the same video with a single global key, because supposedly the POSITA:

would have been motivated to apply this teaching to encrypt all media files, including all alternative representations, using a global key to simplify key management particularly for content that is not particularly sensitive. *Lindahl* teaches that when data “is not that sensitive...the use of a common global key to encrypt such is adequate.”

Pet., 31 (citations omitted).

This statement is unsupported and wrong for multiple reasons. ***First***, as discussed in the immediately preceding section, Lindahl does not teach that “data” in general can be encrypted with a global key when it is not sensitive; rather, Lindahl only teaches that “***metadata***” in a media file should ever be encrypted using a global

key, and even then, only in certain circumstances where the metadata is “not that sensitive.” Ex. 1007 [Lindahl] ¶ 48.

Second, even if Lindahl did teach the concept of using a global key for content which it does not, the Petition does not explain why, if media content were so unimportant that it would be consistent with Lindahl’s teachings to encrypt it using a single global key, the content producer or server would invest the substantial effort of encoding that “not that sensitive” content with multiple alternative bitrates to create multiple alternative streams for it to be viewed by end-users, as opposed to simply utilizing a single stream for low-priority free content. Ex. 1007 [Lindahl] ¶ 48; *compare* Pet. 31; *accord*, e.g., Hurst 19:1-6 (“Encrypt[ing] each bitrate with a different set of encryption keys ... beneficially allows for a publisher to allow a ‘standard’ user to view the movie at a lower resolution while a ‘premium’ user is allowed to watch the movie at a higher resolution or bitrate”). Again, Lindahl is not a system that has multiple alternative streams itself. Ex. 2012 [Nielson Decl.] ¶ 113.

Third, Petitioner’s argument is supported by nothing but a conclusory statement. In particular, Petitioner’s expert claimed that it was “well-known” to use a global key for content that was “low cost or free.” Ex. 1003 [McDaniel Decl.] ¶ 145. Petitioner’s expert, however, provided no evidence, including any article or other scholarly publication, to support his proposition. “[E]xpert testimony,” such as this, “that does not disclose the underlying facts or data on which the opinion is

based is entitled to little or no weight.” 37 C.F.R. § 42.65(a). Thus, the entire basis of Petitioner’s combination is Dr. McDaniel’s conclusory and unsubstantiated testimony that it was “well-known” to use a global key for content that was “low cost or free.” An unsubstantiated assertion such as this cannot establish a motivation to combine as a matter of law.

Moreover, there is no reason to just accept Petitioner’s unsubstantiated contention. For example, when media is broadcast without the need for any restriction (e.g., geographical restriction), it is broadcast as “free-to-air,” which has no encryption whatsoever. Ex. 2020 [Free-to-view]. However, even the otherwise free broadcast does not generally use a global key but would be sent as a “free-to-view” system that would require decryption equipment. *Id.* One prominent user of such a system was BBC (British Broadcast Corporation), which used the VideoGuard system, and which did not allow the use of a global key. *Id.*; *see also* Ex. 2012 [Nielson Decl.] ¶ 114.

The reluctance of a POSITA to use a global key for any reasonable system that would have alternative streams of content in a streaming service as the claims require is also supported by the fact that using a single key to encrypt an entire system would make the entire system compromised with a simple mistake by just one of the many parties involved. For example, in the 1990s, DVDs were encrypted using a global key—until the key was compromised and the entire system was

rendered obsolete.⁵ As one observer noted, a global key system can be compromised in its entirety even where one of the many licensees who use the product inadvertently does not secure the key:

The anonymous developers of the decryption program that removes DVD copy protection had an easy time doing it, thanks to a gaffe by a software developer and the surprising weakness of the encryption technology. Essentially, the two European hackers who developed the DeCSS utility that copies a DVD movie disc were able to break the code because one of the product's licensees inadvertently neglected to encrypt the decryption key.

Ex. 2016 [Patrizio]; *see also* Ex. 2012 [Nielson Decl.] ¶ 115.

Thus, Petitioner's attempt to extend Lindahl beyond its disclosure of encrypting only "not that sensitive" metadata of stored files with a global key, to the encryption of entire multiple adaptive streams of media content from beginning to end with a global key, is supported by nothing but thin air. Moreover, that expansion of Lindahl's teachings would be particularly inappropriate for this critical limitation. The Petition concedes that using common frame encryption keys to encode

⁵ "AACCS is the successor to the Content Scramble System (CSS) [2] used to protect the content on DVDs ... Because CSS provides no mechanism for revoking a compromised key the system has been completely broken since the initial compromise." Ex. 2019 [Henry].

alternative video streams goes to the heart of the claimed invention. *See* Pet., 11 (“According to PO, the ’558 patent is directed to using ‘common frame encryption keys to encode alternative video streams.’”) (internal citation omitted). Petitioner may not use the “common knowledge” of artisans as a “gap-filler” to simply add a claim limitation that is missing from an obviousness combination—especially where the missing limitation goes to the heart of the invention. *DSS Tech. Mgmt. v. Apple Inc.*, 885 F.3d 1367, 1374 (Fed. Cir. 2018); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1363 (Fed. Cir. 2016); *see also infra* Section III.C.⁶

For these reasons, Lindahl does not disclose or suggest encrypting video frames in the alternative streams of content using “a set of common keys.” And even if Lindahl did have such a disclosure, the Petition has not met its burden to show

⁶ The Petition also argues that, in light of Lindahl, there were “finite number” of possibilities: either to use a common set of keys or not to use a common set of keys. Pet., 32. Here, however, Petitioner does not demonstrate that a POSITA, even if aware of the possibility of using a global key or a common set of keys, would be motivated to implement it in a system as claimed.

why a POSITA would combine this alleged suggestion from Lindahl in the system of Chen as proposed.⁷

B. The Petition Fails To Show That Chen In View Of Hurst Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.

The Petition alternatively relies on Hurst for the disclosure of encrypting video frames in alternative streams of content using “a set of common keys.” Pet., 32-33. Hurst, however, only references in passing the fact that the same key *can* be used for all streams, a point that was not in dispute. The question is whether Hurst teaches doing so for alternative streams of protected content, and Hurst teaches against doing such a thing—for Hurst follows its entirely noncommittal mention that it is *possible* to use a single key followed by a prolonged discussion of why it is better to *not* use a single key and to instead use a different specialized

⁷ Moreover, the Petition’s discussion of “Motivation to Combine,” Pet., 17-22, does not appear to allege any motivation to import any alleged use of global key from Lindahl to Chen. Rather, its alleged motivation appears to be exclusively based on importing the concept of common key from Hurst into Chen. *See, e.g.*, Pet., 21 (“For example, a video streaming system would encode multiple representations of a video at different bitrates, as taught by Chen, with the representation partially encrypted as taught by Lindahl, *using common keys, as taught by Hurst.*”).

key for each alternative stream. Thus, Hurst does not provide any reason for a POSITA to use the same key to encrypt alternative streams of protected content to meet the claimed invention. *See* Section IV.B.1. Furthermore, the Petition fails to show legally sufficient motivation as to why a POSITA would combine Chen with Hurst to disclose this limitation. *See* Section IV.B.2.

1. Experts Agree That Hurst Itself Does Not Provide Motivation To Encrypt “Video Frames” Of Alternative Streams Using “A Set Of Common Keys.”

Petitioner relies upon a single sentence in Hurst: “The streamlets 304 of different bitrates may be encrypted with the same key.” Ex. 1008 [Hurst] 18:66-67. That sentence is immediately followed by an explanation of why it would be “beneficial” to instead “encrypt each bit rate with a different set of encryption keys”:

Alternatively, the encoder module 406 may be configured to encrypt each bit rate *with a different set of encryption keys*. *This, beneficially*, allows for a publisher to allow a “standard” user to view the movie at a lower resolution while a “premium” user is allowed to watch the movie at a higher resolution bitrate.

Ex. 1008 [Hurst] 18:64-19:6.

Conspicuously absent from Hurst’s disclosure above is any mention of any benefit to using the same key, as opposed to using different sets of encryption keys. Ex. 2012 [Nielson Decl.] ¶¶ 117. Instead, Hurst unambiguously touts the latter as superior. In fact, Petitioner’s own expert at deposition admitted that he “do[es not]

see an explicit disclosure of an advantage by Hurst.” Ex. 2013 [McDaniel Depo.] 91:20-92:3. Since prior art teaches away when “a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant,” *Allergan, Inc. v. Sandoz Inc.*, 796 F.3d 1293, 1305 (Fed. Cir. 2015), this single sentence in Hurst cannot motivate the POSITA to modify Chen to encrypt alternative streams of protected content with the same key.

It is also notable that there is no disclosure in Hurst to suggest to a POSITA that use of a the same key to encrypt alternate streams of protected video provides adequate security in a system that *also* uses partial frame encryption as disclosed by Lindahl—as both using the same key and partial encryption could negatively impact security. Ex. 2012 [Nielson Decl.] ¶ 118.

As will be discussed below, Petitioner fails to provide any legally sufficient motivation to combine Hurst’s non-committal disclosure of the possibility of using the same key to encrypt alternative streams of video.

2. The Petition’s Fails To Show Any Proper Motivation To Modify Chen In View Of Hurst.

Petitioner’s entire stated motivation to combine *Hurst*’s non-committal disclosure of the possibility of using the same key to encrypt alternative streams with Chen is essentially that because alternative streams of a video may be accessed as a

group, it would be obvious to use the same key to encrypt alternative streams of the video:

POSITA would have been motivated to apply Hurst's teachings—e.g., where the alternative streams are encoded at different bitrates and encrypted as a group in the same manner, such as by using the same key—because they follow the usage model for video distribution in adaptive streaming, where the playback device gains access to the alternative streams as a group. *See id.*; Ex. 1006, ¶¶[0063-0064]; §I.B. For example, a playback device adaptively streaming a movie is typically granted access to its alternative streams for the movie because it is expected to switch between them depending on channel bandwidth. Ex. 1003, ¶116. ***Since the alternative streams are accessed as a group, it would have been obvious to encrypt them as a group, using the same set of keys, so that the alternative streams can be accessed as a group using that set of keys.*** *See id.* Thus, Hurst teaches the natural and obvious approach to DRM for adaptive streaming, which a POSITA would have been motivated to apply. *Id*

Pet., 19, *citing* Ex. 1003 [McDaniel Decl.] ¶ 116.

Petitioner's explanation is conclusory and legally insufficient to establish obviousness on its face. Indeed, it is unclear what the proffered "motivation" even is. Petitioner contends that, "[s]ince the alternative streams are accessed as a group, it would have been obvious to encrypt them as a group, using the same set of keys, so that the alternative streams can be accessed as a group using that set of keys," (Pet., 19) but no explanation is given for why this is beneficial or how any benefits

may outweigh the reduced security of using a single key especially if combined with partial frame encryption, which is already inherently less secure than fully encrypted videos. Ex. 2012 [Nielson Decl.] ¶¶ 119-120.

Petitioner’s conclusory analysis fails as a matter of law. “It is not enough to say that...to do so would ‘have been obvious to one of ordinary skill.’ Such circular reasoning is not sufficient—more is needed to sustain an obviousness rejection.” *Kingston Tech. Co., Inc. v. Polaris Innovations Ltd.*, IPR2016-01622, Paper 7, 15-16 (PTAB Feb. 15, 2017) (citing *In re Chaganti*, 554 Fed. Appx. 917, 922 (Fed. Cir. 2014)); see *Hulu LLC v. Sound View Innovations LLC*, IPR2018-00582, Paper 34, 20-21 (PTAB Aug. 5, 2019) (informative) (rejecting proposed combination where petitioner had not “adequately supported” why it would have been a “good idea” to modify the references as proposed). Notably, as discussed above, Petitioner’s own reference, Hurst, while disclosing the possibility of using the same key, touts the use of different keys to encrypt alternative streams of video. Ex. 1008 [Hurst] 18:64-19:6. Similarly, to the extent that Lindahl utilizes a “global key,” it only teaches using it to encrypt metadata, not video frame, and even then only unimportant metadata. Ex. 1007 [Lindahl] ¶ 48.

To the extent that the Petition is somehow interpreted to implicitly provide any reason why a POSITA would be motivated to use a common set of keys to encrypt alternative streams of the same video, it should be rejected as its proffered

rationale is a restatement of the '588's own teachings. *Compare, e.g.,* Pet., 19 (“so that the alternative streams can be accessed as a group using that set of keys”) *with* Ex. 1001 [’588 Patent] 13:11-21 (“the playback device can use the same cryptographic information to access content in any of the alternative streams of protected content within a single instance of the title.”). Petitioner’s attempt to use the Patent’s own disclosure to show obviousness is improper. *In re Lee*, 277 F.3d 1338, 1344 (Fed. Cir. 2002) (alteration marks omitted, quoting *W.L. Gore v. Garlock, Inc.*, 721 F.2d 1540, 1553 (Fed. Cir. 1983)). “The inventor’s own path itself never leads to a conclusion of obviousness; that is hindsight.” *Otsuka Pharm. Co. v. Sandoz, Inc.*, 678 F.3d 1280 (Fed. Cir. 2012); *accord, e.g., In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999) (“tak[ing] the inventor’s disclosure as a blueprint for piecing together the prior art to defeat patentability” in this manner is “the essence of hindsight.”). In contrast to Hurst and Lindahl, the ’588 Patent provides detailed analysis and discussion on why its system uses a set of common keys despite its drawbacks. *See* Ex. 1001 [’588 Patent] 8:55-61; 10:27-31; 23:46-51.

An invention “composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” *KSR Int’l Corp. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007). For these reasons, the

Petition has failed to meet its burden to show why a POSITA would modify Chen to use a common key either in view of Lindahl or as disclosed in passing by Hurst.

V. CONCLUSION

For the foregoing reasons, Petitioner has failed to demonstrate that any of the claims are unpatentable.

Respectfully submitted,

_____/ Kenneth J. Weatherwax /_____

Kenneth J. Weatherwax, Reg. No. 54,528
Lowenstein & Weatherwax LLP

Date: December 7, 2020

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Response (the “POR”) consists of 13,239 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The POR complies with the type-volume limitation of 14,000 words as mandated in 37 C.F.R. § 42.24. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Respectfully submitted,

/ Parham Hendifar /

Date: December 7, 2020

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served by electronic service, by consent between the parties (Pet. at 85), on the date signed below:

PATENT OWNER DIVX LLC'S RESPONSE TO PETITION FOR INTER PARTES REVIEW OF UNITED STATES PATENT NO. 10,225,588

EXHIBITS 2012-2020

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

HBatts@sheppardmullin.com,
CPonder@sheppardmullin.com,
JLiang@sheppardmullin.com,
LegalTm-DivX-IPR@sheppardmullin.com

Respectfully submitted,

/ Patrick Maloney /

Date: December 7, 2020