

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case IPR2024-00215
Patent 10,452,854

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

	Page
I. THE BOARD SHOULD DISREGARD THE IMPROPERLY-INCORPORATED REPLY-DECLARATION AND NEW EXHIBITS.....	1
II. FOSTER-HAYHURST FAILS (GROUND 2, ALL CLAIMS).	2
A. Petitioner Fails To Prove Hayhurst Is Analogous Art (Ground 2, All Claims).	2
B. Failure To Demonstrate Motivation To Combine (Ground 2, All Claims).	5
1. Undisputed: Foster-Hayhurst Would Thwart Foster’s Fundamental Aims.	6
2. Petitioner Improperly Changes Its Unpatentability Theory.	10
3. Petitioner’s New Theories Are Meritless.....	14
C. “Generating A Plurality Of Data Chunks Based On The Data Set” By “Distributing The Data Set Into A Plurality Of Shares” (Ground 2, All Claims).....	17
III. ORSINI FAILS (GROUND 1, ALL CLAIMS).	19
IV. CONCLUSION.....	26

TABLE OF AUTHORITIES**Page(s)****COURT DECISIONS**

<i>ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	24
<i>Arctic Cat Inc. v. Polaris Indus.</i> , 795 Fed. App'x. 827 (Fed. Cir. 2019)	10
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	12, 13
<i>Donner Tech., LLC v. Pro Stage Gear, LLC</i> , 979 F.3d 1353 (Fed. Cir. 2020)	4
<i>Henny Penny Corp. v. Frymaster LLC</i> , 938 F.3d 1324 (Fed. Cir. 2019)	12
<i>Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	1
<i>Medtronic, Inc. v. Teleflex Innovations S.A.R.L.</i> , 70 F.4th 1331 (Fed. Cir. 2023)	26
<i>Netflix, Inc. v. DivX, LLC</i> , 80 F.4th 1352 (Fed. Cir. 2023)	3
<i>Netflix, Inc. v. DivX, LLC</i> , 84 F.4th 1371 (Fed. Cir. 2023)	14
<i>Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.</i> , 97 F.4th 882 (Fed. Cir. 2024)	21
<i>Yita LLC v. MacNeil IP LLC</i> , 69 F.4th 1356 (Fed. Cir. 2023)	12

AGENCY DECISIONS

Cisco Sys., Inc. v. C-Cation Tech., LLC,
IPR2014-00454, Paper 12 (Aug. 29, 2014)
(informative) 2

Edwards Lifesciences Corp. v. Aortic Innovations LLC,
IPR2023-01232, Paper 10 (Feb. 7, 2024) 21

Samsung Austin Semiconductor, LLC v. Red Rock Analytics, LLC,
IPR2018-00556, Paper 18 (Aug. 20, 2018) 24

REGULATIONS

37 C.F.R. §42.6(a)(3) 2

OTHER AUTHORITIES

Consolidated Trial Practice Guide 1

EXHIBIT LIST	
2001	Declaration of Nathan Lowenstein in Support of Motion for <i>Pro Hac Vice</i> Admission
2002	Declaration of Colette Woo in Support of Motion for <i>Pro Hac Vice</i> Admission
2003	Declaration of Aviel D. Rubin, Ph.D.
2004	Reserved
2005	Bruce Schneier Curriculum Vitae [Schneier-CV]
2006	Bruce Schneier, <i>Why Cryptography Is Harder Than It Looks</i> , SCHNEIER ON SECURITY, 1997, https://www.schneier.com/essays/archives/1997/01/why_cryptography_is.html [Schneier-Why-Cryptography-Is-Harder-Than-It-Looks]
2007	Excerpts from Jonathan Katz et al., <i>Introduction to Modern Cryptography</i> (1st ed. 2007) [Katz]
2008	Bruce Schneier, <i>Security Pitfalls in Cryptography</i> , SCHNEIER ON SECURITY, 1998, https://www.schneier.com/essays/archives/1998/01/security_pitfalls_in.html [Schneier-Security-Pitfalls-in-Cryptography]
2009	Excerpts from Ross Anderson, <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i> (1st ed. 2001) [Anderson]
2010	Excerpts from Bruce Schneier, <i>Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C</i> (2nd ed. 2015) [Schneier-Applied-Cryptography]
2011	Patent Application Publication to Tsai US 2005/0195857 A1 [Tsai]
2012	Edgar Pek et al., <i>Formal Verification of Communication Protocols in Distributed Systems</i> , SYMPOSIUM ON OPERATING SYS. PRINCIPLES, 2003 [Pek]

2013	Jan Friso Groote et al., <i>A Bounded Retransmission Protocol for Large Data Packets: A Case Study in Computer Checked Algebraic Verification</i> , 1996 [Groote]
2014	Microsoft, <i>Overview of MPEG-2 Systems</i> , WWW.LEARN.MICROSOFT.COM , July 27, 2023, https://learn.microsoft.com/en-us/windows/win32/directshow/overview-of-mpeg-2-systems [Overview-of-MPEG-2-Systems]
2015	Excerpts from Harry Newton, <i>Newton's Telecom Dictionary</i> (16th ed. 2000) [Newton's-Telecom-Dictionary]
2016	Excerpts from <i>Oxford Dictionary of Computing</i> (1996) [Oxford-Dictionary-of-Computing]
2017	IBM, <i>Transmission Control Protocol (TCP)</i> , WWW.IBM.COM , https://www.ibm.com/docs/en/zos-basic-skills?topic=4-transmission-control-protocol-tcp [IBM]
2018	<i>Security First Innovations, LLC v. Google LLC</i> , 2:23-cv-00091 (JKW-RJK), Google's Opening Claim Construction Brief (December 6, 2023) [Google's-Opening-Claim-Construction-Brief]
2019	Excerpts from Microsoft Press, <i>Microsoft Computer Dictionary</i> (5th ed. 2002) [Microsoft-Computer-Dictionary]
2020	<i>Security First Innovations, LLC v. Google LLC</i> , 2:23-cv-00091 (JKW-RJK), Google's Responsive Claim Construction Brief (Jan. 8, 2024) (Non-Confidential Redacted Version) [Google-Responsive-Claim-Construction-Brief]
2021	Cambridge Dictionary, <i>Set-Top Box</i> , https://dictionary.cambridge.org/us/dictionary/english/set-top-box (last visited Feb. 27, 2024)

2022	Jim Connors, INFOWORLD, <i>The evolution of cable television to interactive communications service provider</i> (Oct. 1, 1996), https://www.infoworld.com/article/2077255/the-evolution-of-cable-television-to-interactive-communications-service-provider.html [InfoWorld]
2023-2027	Reserved
2028	Declaration of Colette Woo [SERVED, NOT FILED]
2029	Jonathan Katz et al., <i>Introduction to Modern Cryptography</i> (1st ed. 2007) [SERVED, NOT FILED]
2030	Reserved
2031	Ross Anderson, <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i> (1st ed. 2001) [SERVED, NOT FILED]
2032	Bruce Schneier, <i>Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C</i> (2nd ed. 2015) (E-Book) [SERVED, NOT FILED]
2033	Second Declaration of Aviel D. Rubin, Ph.D. [Rubin-2 nd -Decl.]
2034	Deposition Transcript of Samrat Bhattacharjee [Bhattacharjee-Depo.]
2035	C. Patrikakis et al., <i>Streaming Content Wars: Download and Play Strikes Back</i> , UCMedia 2009, LNICST 40, pp. 218–226, 2010. [Patrikakis]
2036	J. Hur et al., <i>Packet Chunking for File Detection</i> , IEEE/ACM Transactions on Networking Vol. 31 (2023). [Hur]
2037	R. Li et al., <i>A Framework for Qualitative Communications Using Big Packet Protocol</i> , 2019, https://doi.org/10.48550/arXiv.1906.10766 . [Li-I]

2038	N. McKeown et al., <i>The Tiny Tera: A Packet Switch Core</i> , IEEE Micro 17, 1998. [McKeown]
2039	<i>Marlin DRM FAQ</i> , Marlin Community, https://www.marlin-community.com/faq/ (last accessed Sept. 9, 2024) [Marlin-DRM]
2040	<i>What is Conditional Access?</i> , Verimatrix anti-piracy (Aug. 1, 2023), https://www.verimatrix.com/anti-piracy/knowledge-base/what-is-conditional-access/ [Verimatrix]
2041	R. Li et al., <i>New IP: A Data Packet Framework to Evolve the Internet</i> , 2020, https://www.researchgate.net/publication/341582478 [Li-II]
2042	Vimal Kumar et al., <i>POP: Privacy and Integrity Preserving Data Aggregation in Wireless Sensor Networks</i> , PROCEEDINGS OF THE IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS, September 2013 [Kumar]
2043	Yuxin Mao et al., <i>A Feedback-Based Secure Path Approach for Wireless Sensor Network Data Collection</i> , SENSORS, October 22, 2010 [Mao]
2044	Institution Decision in IPR2024-00215 [215-ID]
2045	Second Declaration of Colette Woo [SERVED, NOT FILED]
2046	Second Deposition Transcript of Samrat Bhattacharjee [Bhattacharjee-2 nd -Depo.]

Petitioner’s Reply confirms that Petitioner did not “make [its] case in [its] petition.” *Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016). Had Petitioner made its case, it would have hardly needed a **111-page, 29,000-word Reply declaration** and **43 new exhibits** to attempt to fill the Petition’s numerous holes. This new evidence, in support of new arguments, should not be considered. CTPG, 73 (“Petitioner may not submit new evidence or argument in reply that it could have presented earlier, e.g. to make out a prima facie case of unpatentability.”). Even if that could be overlooked, its unexplained citations to the reply-declaration constitute improper incorporation by reference (Section I) and further fail to demonstrate that any of the challenged claims are invalid (Sections II-III). The claims should be confirmed.

I. THE BOARD SHOULD DISREGARD THE IMPROPERLY-INCORPORATED REPLY-DECLARATION AND NEW EXHIBITS.

The reply-declaration and the new exhibits are improperly incorporated by reference and should be disregarded. The Reply does not meaningfully discuss hardly any of the reply-declaration’s 256 paragraphs. The Reply’s *modus operandi* is to include a conclusory sentence purportedly “supported” by citations to up to 22 paragraphs of Dr. Bhattacharjee’s reply-declaration. *E.g.*, Reply, 18 (citing ¶¶157-179); 11 (citing ¶¶89-105); 9 (citing ¶¶74-85); 21 (citing ¶¶200-210); 7 (citing ¶¶48-57); 29 (citing ¶¶245-254). The Reply similarly includes unexplained

citations to 43 new exhibits. *E.g.*, Reply, 9 (unexplained citations to new exhibits 1073, 1097, 1075, 1077, 1092). This is impermissible incorporation by reference, and the unexplained citations to the reply-declaration and new exhibits should be disregarded. 37 C.F.R. §42.6(a)(3); *Cisco Sys., Inc. v. C-Cation Tech., LLC*, IPR2014-00454, Paper 12, 9-10 (Aug. 29, 2014) (informative).

II. FOSTER-HAYHURST FAILS (GROUND 2, ALL CLAIMS).

A. Petitioner Fails To Prove Hayhurst Is Analogous Art (Ground 2, All Claims).

Petitioner has the burden of proving Hayhurst is analogous art and did not attempt to carry that burden in the Petition. POR, 32-41. The Reply fares no better. To meet its burden, Petitioner was required to identify the field of endeavor to which the '854 relates, and the problem or problems that Hayhurst attempted to solve. POR, 33 (citing cases). Petitioner declined to do either. Reply, 2, 5-6; Ex. 1111 [Bhattacharjee-2nd-Decl.] ¶11 ("I have not been asked to opine on whether SFI has identified the correct field of endeavor for the '854 patent."); Ex. 2046 [Bhattacharjee-2nd-Depo.] 102:3-103:13 (Dr. Bhattacharjee did not determine field of endeavor); *see also* Reply, 5-6 (not identifying problem Hayhurst sought to address); Ex. 1111 [Bhattacharjee-2nd-Decl.] ¶¶27-47 (same). Thus, the Reply cannot rectify Petitioner's failure to carry its burden.

If more is needed, the '854 and Hayhurst do not share the same field. POR, 33-37; Ex. 2033 [Rubin-2nd-Decl.] ¶¶102-104. The '854's field is securing data, while Hayhurst's field is decentralized media delivery. The Reply does not dispute the '854's field but attempts to identify Hayhurst's field by its reference to "secure handling and storage." Reply, 2 (discussing Ex. 1007, [0002]). Petitioner, however, ignores the immediately preceding clause which states: "[t]his application relates to **the field of electronic media delivery, such as video-on-demand** ..." Ex. 1007, [0002].

Petitioner similarly ignores that each of Hayhurst's title, abstract, technical field, background, summary, specification/figures, and claims—the traditional sources used to discern the field of endeavor—**all** confirm that Hayhurst's field is "decentralized media delivery." See POR, 34-36. Ignoring Patent Owner's discussion of each of these sources, Petitioner attacks a strawman, contending that the field is not discerned from the problem the reference tries to address. Reply, 4 (citing *Netflix, Inc. v. DivX, LLC*, 80 F.4th 1352, 1359 (Fed. Cir. 2023)).

Petitioner tries to sidestep Patent Owner's argument by asserting that that "decentralized media delivery" "is how Hayhurst provides 'security and [] deterrence to piracy' of stored data." Reply, 3. But this gets Hayhurst backwards; security and deterrence to piracy is merely a by-product of Hayhurst's decentralized media delivery, which seeks to overcome bandwidth inefficiencies

associated with prior art video-on-demand systems via a decentralized video-on-demand system. Ex. 1007 [Hayhurst] [0004]-[0006]. Solely as a by-product, the “segmented and distributed storage of the media file” can provide an additional “level of security and a deterrence to piracy.” *Id.*, [0008]. But Hayhurst’s focus is achieving a “decentralized approach to delivering a media file.” POR, 35-36 (discussing Ex. 1007, Title, Abstract, [0002], [0003]-[0004], [0005], [0012], [0015]).

As for the reasonable pertinence prong, “when addressing whether a reference is analogous art with respect to a claimed invention under a reasonable-pertinence theory, ***the problems to which both relate must be identified and compared.***” *Donner Tech., LLC v. Pro Stage Gear, LLC*, 979 F.3d 1353, 1359 (Fed. Cir. 2020). Neither the Petition nor the Reply identify the problem Hayhurst sought to solve or compare it to the problem solved by the ’854.

And Petitioner cannot dispute Hayhurst’s plain statement that its “invention addresses ***the problem*** of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files.” Ex. 1007 [Hayhurst] [0004]-[0005]; POR, 39-40; Ex. 2033 [Rubin-2nd-Decl.] ¶107. Petitioner does not dispute that Hayhurst’s limited bandwidth problem is not reasonably pertinent to the ’854’s problem of eliminating user-related vulnerabilities in storing sensitive information, nor does it contend that limited

bandwidth is reasonably pertinent to any “additional” problems Petitioner purports the ’854 addresses. POR, 40-41; Ex. 2033 [Rubin-2nd-Decl.] ¶¶108-109; Reply, 5-6.

B. Failure To Demonstrate Motivation To Combine (Ground 2, All Claims).

The POR demonstrated Petitioner’s failure to prove a motivation to combine Foster and Hayhurst. POR, 41-62. The Reply confirms that failure.

First, Petitioner does not dispute that Foster is concerned with reducing delays, particularly in the live television/streaming context or that Foster-Hayhurst would frustrate Foster’s goals by greatly increasing the delays Foster sought to avoid and render Foster unsuitable for live television/streaming. *See* Section II.B.1.

Second, implicitly admitting that a POSITA would not be motivated to make its originally-proffered combination, Petitioner shifts to a new combination, arguing for the first time that Foster-Hayhurst is limited to Foster’s alleged “storage context,” something not even mentioned in the Petition. In the Petition, *all* of Foster’s content units are stored and distributed using *Hayhurst’s* decentralized delivery method. The Reply, by contrast, relies on new theories and purported evidence to argue that Foster’s storage method should also be used, in order to manufacture a motivation to combine Foster-Hayhurst. Under governing

precedent, Petitioner's untimely new theory should not be considered. See Section II.B.2. Even if considered, Petitioner's new argument should be rejected. See Section II.B.3.

1. Undisputed: Foster-Hayhurst Would Thwart Foster's Fundamental Aims.

The Petition's Foster-Hayhurst combination involved storing "Foster's encrypted content units" "on multiple storage devices ... based on Hayhurst's techniques for storing and distributing encrypted data segments" of a media file. POR, 49 (citing Pet., 61). Notably, Petitioner's combination applied to all of "Foster's encrypted content units" without regard to any particular context. POR, 49-50 (citing Pet., 61-64; Ex. 2034 [Bhattacharjee-1st-Depo.] 126:3-9).

The POR explained that the proposed Foster-Hayhurst combination would undermine Foster's fundamental aims. POR, 41-62. Whereas Foster is directed towards reducing delays experienced by a user when randomly accessing content because encrypted packets and encryption keys are not synchronized, the proposed combination would introduce substantial, far greater delays than those Foster sought to avoid. *Id.*, 42-49.

Foster's emphasis is upon avoiding delays to allow for swift random access to content. As Petitioner's expert concedes, "synchronous transmission" of a series of packets and the keys used to encrypt them to a single receiver to "foster random

access to content” was “sort of the whole invention in Foster.” Ex. 2034 [Bhattacharjee-Depo.] 32:20-23. The Foster-Hayhurst combination, however, would thwart these aims. Rather than stream a movie to a subscriber for immediate viewing, Hayhurst’s distribution method requires the movie to be divided into segments across thousands of households. When a household requests a movie, its set top box (“STB”) must, *inter alia*, receive and recombine all of the segments before the movie can be displayed. POR, 49-51. Applying Hayhurst’s distribution regime to Foster would massively increase delays (the very thing Foster sought to avoid) and preclude real-time streaming and/or random access to content. *Id.*, 49-63. And the synchronization of keys and content required by Foster is irrelevant to Hayhurst. *Id.*, 47-49.

In reply, Petitioner does not dispute that Foster is principally directed towards reducing delays, facilitating random access to content, and live streaming. Instead, Petitioner argues that Foster is not “limited [to streaming live broadcasts] and also concerns storing secured data.” Reply, 10. But Patent Owner’s argument has never been that Foster is “limited to streaming live broadcasts.” Rather, the POR demonstrated that Foster seeks to improve upon prior-art systems (DRMS and CAS) used for live or real-time television/streaming by synchronizing content packets and the keys used to encrypt each packet. POR, 55-56; *see also* Ex. 1006 [Foster] [0006]-[0007], [0050], [0052].

While Petitioner does dispute the POR's showing that Foster-Hayhurst would undermine Foster's security, that argument also fails. As the POR explained, Foster-Hayhurst should additionally be rejected because Hayhurst's method would compromise the security of Foster's system as Foster's key-encryption-keys ("KEKs") would be more vulnerable and Foster's ability to change KEKs as necessary would be eliminated. POR, 58-61. In reply, Petitioner downplays the importance of the ability to change KEKs to Foster's security, arguing that "Foster recognizes 're-encrypting the content itself,' rather than changing the KEK, is an alternative." Reply, 11. Wrong. Foster specifically teaches "an encrypted title key 30 can be re-encrypted with a different key encrypting key 32 ***without having to re-encrypt the encrypted content 26***" "***which could be significantly more time-consuming and/or consume more resources than re-encrypting title key 24.***" Ex. 1006 [Foster] [0054]; see Ex. 2046 [Bhattacharjee-2nd-Depo.] 25:21-27:10 ("reencrypting a content would be more time-consuming than reencrypting a key."). Thus, Petitioner's contention is contrary to Foster's teachings.

Petitioner also argues, without explanation, that "POSAs knew how to change/replace KEKs across many devices/users." Reply, 11-12 (citing new Exhibits 1078-1080). This argument exemplifies why Petitioner's unexplained citations to new references should be rejected. Aside from being untimely, none of

the newly cited exhibits involve changing/replacing KEKs, much less across many devices/users. *See* Ex. 1078, 4:5-28 (concerning information delivery method in peer-to-peer network, not KEKs); Ex. 1079, 544-546 (replacing session keys, not KEKs); Ex. 1080, 2-7 (replacing traffic encryption keys, not KEKs).

Petitioner does not dispute that Foster-Hayhurst, by distributing KEKs among thousands of subscribers, would compromise the security of the combination as compared to Foster alone. POR, 58-61. In reply, Petitioner side-steps the point, arguing for the first time that “Foster-Hayhurst would not store a KEK on user devices” because “[a]s in Foster alone, users could only access a KEK once authorized to decrypt the content.” Reply, 12 (citing Ex. 1006, [0049], [0052]). Petitioner, however, cites Foster’s description of prior-art, rather than Foster’s system. Ex. 1006 [Foster] [0049], [0052] (describing prior-art DRMS); *see also* Section II.B.3. In Foster’s actual invention, the KEK is delivered to the user device “**prior to**[] the encrypted content.” *Id.*, [0056]. Moreover, even if (contrary to Foster’s teachings), Foster-Hayhurst only delivered the KEK to authorized users, that would still leave the KEKs far more exposed. It is undisputed that in these circumstances, Foster’s KEKs can no longer be unique to a user and are, at most, unique to a movie. POR, 59-61. Thus, rather than having only one copy of a KEK exposed, as many KEK copies are exposed as there are reassembled content files. *Id.*

In sum, the POR’s showing that a POSITA would not be motivated to combine Foster-Hayhurst is un rebutted. Again, “[t]he Board must weigh the benefits and drawbacks of the modification against each other, to determine whether there would be a motivation to combine.” *Arctic Cat Inc. v. Polaris Indus.*, 795 Fed. App’x. 827, 833 (Fed. Cir. 2019); POR 51, 24-25 (citing additional cases). Petitioner does not dispute that the Board must weigh the benefits and drawbacks, does not perform any such weighing in its Reply, and does not dispute Patent Owner’s showing that the numerous drawbacks described in the POR outweigh the benefits alleged in the Petition. *See* Reply, 7-13. Consequently, Patent Owner’s demonstration that the drawbacks to Petitioner’s proposed combination outweigh any alleged benefits remains unchallenged.

2. Petitioner Improperly Changes Its Unpatentability Theory.

The Reply also impermissibly changes the structure of the Foster-Hayhurst combination from that described in the Petition. In its Reply, for the first time, Petitioner argues that its combination relies on Foster’s “storage context” rather than on Hayhurst’s method for storing encrypted data segments on multiple distributed storage devices. *See* Reply, 7. Specifically, Petitioner argues that “Foster’s teachings are not limited to live-streaming” as “Foster teaches storing encrypting content for and by recipient(s) (*e.g.*, video-on-demand).” *Id.* Petitioner

then argues that in “Foster’s storage context,” “POSAs would have recognized the benefits of combining Foster with Hayhurst.” *Id.*

But the Petition did not rely upon “Foster’s storage context.” The Petition never mentions “Foster’s storage context,” and it is certainly not the foundation of the Foster-Hayhurst combination. Rather, in the Petition’s Foster-Hayhurst combination, **all** of Foster’s content units are stored and distributed per *Hayhurst’s* decentralized storage/delivery method. POR, 49-50 (discussing Pet., 61-64).

The Reply wrongly asserts that Foster’s storage context was “relied upon in the Petition,” citing the Petition at “65, 80-82.” See Reply, 7. But these pages do not evidence any reliance upon Foster’s “storage context”; they do not even mention it. See Pet., 65, 80-82. Rather, the Petition at 65 argued that “Foster-*Hayhurst*” allegedly “performs a ‘method for securely storing a data set,’” but only relied on “Foster’s method for **securing** digital content,” not **storing** such content. *Id.*, 65. Instead, the Petition expressly relied upon “*Hayhurst’s method for storing* encrypted data segments on multiple distributed storage devices.” *Id.*, 63. The Petition at 80-82 argued that in *Foster-Hayhurst*, “each ‘processed content unit 116’ is stored on a receiver at a different ‘recipient 430’” per Hayhurst’s decentralized regime. In short, the Petition’s Foster-Hayhurst combination relied on Hayhurst’s storage methods, not Foster’s.

Petitioner’s improper shifting of its theory of unpatentability to rely on Foster’s “storage context” demonstrates that it failed to carry its burden in the Petition. Its new arguments should be rejected. *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1368 (Fed. Cir. 2015) (rejecting shift from “a generic statement in Dhallan that any sequencing method can be used” to reliance upon previously unidentified “specific embodiments of Dhallan that do not use restriction-enzyme digestible primers”); *see also Yita LLC v. MacNeil IP LLC*, 69 F.4th 1356, 1367 (Fed. Cir. 2023) (rejecting argument where petitioner, “as the ‘master of its complaint,’ could have ‘present[ed] [its reply] argument in its petition[] but chose not to.’”); *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1330-31 (Fed. Cir. 2019) (“an IPR petitioner may not raise in reply ‘an entirely new rationale’ for why a claim would have been obvious.”).

Petitioner also improperly relies for the first time upon Foster’s alleged and previously-uncited “storage-based purposes,” which, in any event, does not provide a motivation to combine Foster-Hayhurst. In reply, Petitioner newly relies upon a purported “Foster[] DRMS” embodiment as evidence that content is “downloaded to [i.e., stored to a] personal computer’ for on-demand access.” Reply, 8-9. The Petition, however, never mentions any DRMS embodiment, much less storage on a PC. *See, e.g., Pet.*, 80 (Foster-Hayhurst allegedly stores content units on a “consumer set-top box”). Critically, the Petition never mentions

“Foster’s DRMS” because it does not exist; as discussed below: the DRMS depicted in Foster is prior art Foster improved on, not an embodiment of Foster’s inventive system. Section II.B.3. That Petitioner must abandon Foster’s system in favor of Foster’s prior art confirms that the Petition itself did not establish a motivation to combine Foster-Hayhurst.

In support of its pivot, the Reply also argues that “Foster includes storage-based embodiments,” relying upon Foster’s description of “an MPEG ‘program stream,’ which Foster says (and POSAs knew) is intended for storing ‘in fixed storage.’” Reply, 9. But the Petition does not mention, much less rely on, storing an MPEG program stream. *See Pet., generally*. Instead, the Petition relies entirely on “Hayhurst’s techniques for storing and distributing encrypted data segments.” Pet., 61. Hayhurst teaches such segments are distributed through a cable network, and Foster teaches, in that context, that **transport** streams rather than program streams are used. Ex. 1006 [Foster] [0073] (“A transport stream is typically used in error-prone broadcast environments such as digital television.”); Ex. 2046 [Bhattacharjee-2nd-Depo.] 30:16-31:10 (digital television includes cable and satellite). Program streams are thus irrelevant to Petitioner’s original combination.

Petitioner’s reliance on additional, previously unidentified sections of Foster should be rejected. It is improper to cite previously unidentified portions of a prior-art reference to make new arguments. *Ariosa*, 805 F.3d at 1368 (affirming

Board’s “rejection of Ariosa’s reliance, in its Reply submissions, on previously unidentified portions of a prior-art reference to make a meaningfully distinct contention.”); *Netflix, Inc. v. DivX, LLC*, 84 F.4th 1371, 1381-82 (Fed. Cir. 2023) (“It was reasonable for the Board to consider only the theory encapsulated in the plain words of [petitioner’s argument] and decline to discern another theory from the citations alone.”).

3. Petitioner’s New Theories Are Meritless.

Even if they could be considered, Petitioner’s new arguments should still be rejected. As discussed, Petitioner’s Reply argues that its proposed combination constitutes an improvement to the “storage context” described in connection with a purported DRMS embodiment in Foster. Petitioner claims that this purported embodiment involves storing an entire content file on a personal computer for later on-demand viewing. See Reply, 8 (“In Foster’s DRMS, ‘content is packaged and loaded [i.e., stored] onto a web server’ and subsequently ‘downloaded to [i.e., stored to a] personal computer’ for on-demand access (i.e., viewing stored content whenever the user wants to).”). Petitioner’s new argument fails for multiple reasons.

As an initial matter, Petitioner fails to demonstrate that Foster’s inventive system stores a content file on a personal computer. Petitioner relies upon what it claims is “Foster’s DRMS,” as depicted in Foster’s Figure 1. Reply, 8-9. But this

is not “Foster’s” invention; rather, the DRMS Petitioner points to is Foster’s prior art. *See* Reply, 8-9; Ex. 1006 [Foster] [0005] (in “Background Art,” “Current technologies ... include a personal computer-based Digital Rights Management System (DRMS)”), [0049] (in “FIG. 1, a depiction of a Digital Rights Management System (DRMS) is shown.”), Fig. 1. Foster criticizes “the DRMS” depicted in Figure 1 (Ex. 2046 [Bhattacharjee-2nd-Depo.] 24:15-25) because it “fails to provide synchronized delivery of the content with the keys used to encrypt the content”—which, as Petitioner’s expert admits, is “sort of the whole invention in Foster.” Ex. 1006 [Foster] [0051]; Ex. 2034 [Bhattacharjee-1st-Depo.] 32:20-23. Foster’s inventive system is intended to replace both DRMS and CAS. *See id.*, [0003]-[0007] (criticizing DRMS and CAS, concluding a need exists for a system “for synchronized transmission”).

Figure 1’s DRMS is, therefore, a prior-art system that lacks Foster’s invention; it is not an embodiment of or foundation for Foster’s invention. Thus, whether DRMS allegedly stores an entire content file on a personal computer has no bearing on whether Foster’s system does so. And to the extent that Petitioner proposes modifying Foster to use DRMS, Petitioner fails to explain why a POSITA would have been so motivated, especially in view of Foster’s criticism of DRMS.

Nor does Petitioner explain how the *personal computer* used in DRMS would have a place in Foster-Hayhurst which, again, utilizes Hayhurst’s

decentralized distribution system for **set-top boxes**. Pet., 61. Petitioner provides no explanation for what precisely its revised combination would be, why a POSITA would be motivated to make it, much less with a reasonable likelihood of success.

Petitioner also contends that Foster describes an MPEG program stream used for fixed storage. That a content file may be stored in “fixed storage” does not indicate that Foster teaches that the entire content file is stored on a personal computer in its system. Rather, the only embodiment in Foster that Petitioner alludes to as teaching “fixed storage” is “content stored on a DVD.” See Reply, 8. But Petitioner never relied on Foster’s DVD embodiment in the Petition. See Pet., *generally*. And the DVD embodiment cannot apply to the proposed Foster-Hayhurst combination because DVDs do not have a bandwidth problem, nor can they be split amongst set-top boxes via Hayhurst’s scheme.

Petitioner also argues that CAS is not limited to live broadcasting and that in video-on-demand CAS systems, “content is stored pre-encrypted on **hard drives in the VOD server**” and in “**storage media** in which the delivered content can be stored.” Reply, 9 (citing 11 paragraphs of reply-declaration and six new exhibits). Regardless, Petitioner does not dispute that live broadcasting is an essential part of CAS, and Petitioner’s combination would, undisputedly, preclude it. Moreover, Petitioner’s additional evidence still does not demonstrate that Foster’s system

stores an entire content file on the set-top box as Petitioner implies. *See* Reply, 9 (content can be stored on “VOD server” or generic “storage media.”). And, even if it did, Petitioner does not explain why this fact would motivate a POSITA to make Foster-Hayhurst.

**C. “Generating A Plurality Of Data Chunks Based On The Data Set”
By “Distributing The Data Set Into A Plurality Of Shares”
(Ground 2, All Claims).**

The POR explained that Petitioner’s argument that Foster’s teaching of packetizing content per the MPEG protocol does not teach “generating a plurality of data chunks based on the data set” by “distributing the data set into a plurality of shares.” POR, 63-71. The ’854 describes several examples of how to generate shares and makes clear that packets or their payloads are not chunks or shares. *Id.*, 66-69. Indeed, the ’854 identifies a data packet or its packet payload as the dataset to be divided into shares. *Id.*, 67-68 (discussing Ex. 1001 [’854] 82:21-24, 81:36-37, 81:54-58). The ’854’s usage of “chunks” and “shares” as distinct from “packets” or their payloads is consistent with numerous technical articles that refer to a packet or packet payload being split into chunks or shares. *Id.*, 66-67 (citing Exs. 2012-2013, 2036-2038, 2041-2043). The POR further explained that the difference between the ’854’s chunks/shares and Foster’s packets/payloads is significant as the ’854’s data chunks or shares are generated to further secure the

data, and Foster's packet payloads merely exist as a by-product of the MPEG standard. *Id.*, 68-69.

In reply, Petitioner does not dispute the '854's clear teaching that packets or packet payloads themselves are split into chunks or shares. *See* Reply, 13-16. Petitioner ignores these portions and alleges that "SFI suggests a share must be 'cryptographically generated' so the splitting of the data set by itself makes it less susceptible to 'attack.'" *Id.*, 15. But, as seen above, this is not and has never been Patent Owner's position. Rather, the '854's specification gives several examples of how a dataset may be split and is clear that a packet or its payload is itself a dataset that is split into shares or chunks, regardless of whether the split is performed cryptographically. Ex. 1001 ['854] 82:21-24, 81:36-37, 81:54-58.

Petitioner argues that the '854 does not exclude MPEG packetization because the '854 says "any other suitable parsing and splitting approach may be used to generate portions of data from an original data set." Reply, 14-15 (quoting Ex. 1001, 74:56-75:10). But Petitioner never argues that or explains why Foster's MPEG packetization is a "parsing and splitting approach," let alone a "suitable" one. *See id.* Petitioner contends that "Foster's payloads 'are generated to further secure the data' [], because each is encrypted with a different key." *Id.*, 15. But this misapprehends to purpose of packetization which, as both experts agree, is a part of the MPEG standard. Ex. 2046 [Bhattacharjee-2nd-Depo.] 34:2-20, 35:23-

36:15 (MPEG packetization for “optimiz[ation]” such as “random access”).

Petitioner, moreover, never argued that encryption is part of MPEG packetization.

See Reply, 15. Indeed, Petitioner argued that Foster’s encryption of the shares teaches “encrypting each of the shares” rather than “distributing the data set into a plurality of shares.” Pet., 74-75, 77. Petitioner thus fails to rebut the POR’s showing that MPEG packets are not generated to secure data. POR, 68-69.

Finally, Petitioner argues that the POR’s literature demonstrating a known distinction between packets and/or their payloads and chunks/shares is not relevant as they do not relate to MPEG packets. Reply, 16. But the POR’s literature discusses data packets and MPEG packets are a type of data packet. Ex. 2011 [Tsai] [0001]. Petitioner fails to provide any evidence showing that an MPEG packet/payload or any other type of packet/payload is terminology used to refer to a share/chunk. The POR’s showing is thus un rebutted.

III. ORSINI FAILS (GROUND 1, ALL CLAIMS).

As the Board correctly found, Petitioner’s Orsini ground failed even the low bar for institution, finding that Petitioner failed to adequately explain how or why a POSITA would modify Orsini to obtain the claimed inventions. POR, 1-32; ID, 25-39. Rather than defend its positions, Petitioner abandons everything but “one obviousness argument.” Reply, 17. Even then, the Reply only confirms the Petition’s shortcomings.

Abandoning anticipation, the Reply only contends a POSITA would have found it obvious to modify Orsini to encrypt the encryption keys with a public KEK allegedly found in another Orsini embodiment. Reply, 17; Pet., 43-44. The Board, however, has already found that Petitioner failed to sufficiently demonstrate this theory in the Petition. ID, 35-39 (“Petitioner does not provide a sufficient rationale for combining these multiple embodiments.”).¹

Nothing in the Reply rebuts the POR’s demonstration that a POSITA would not be motivated to modify Orsini to use a KEK to “further secure the data chunks,” because Orsini already includes a technique for doing so that is non-cryptographic and not based on any key. *Id.*, 21-24. Nor does the Reply remedy Petitioner’s failure to address how to manage or secure the KEK, or any way of managing the security vulnerabilities its proposed modification would introduce into Orsini’s system. *Id.*, 24-28. As the Board found, Petitioner’s arguments were driven by hindsight. *Id.*, 28-32.

¹ Undisputedly, “performing an encryption operation based on the external key to further secure the plurality of data chunks” involves complex technology and goes to “the heart of [the claimed] invention,” and thus, a court’s review of any purported “reasoned basis for resort to common sense” must be especially “searching.” POR, 19-21.

Instead, Petitioner's Reply introduces new theories and untimely evidence to attempt to fill the Petition's holes. *E.g.*, Reply, 23 (citing new Exhibits 1093, 1106 to newly argue POSITA would have modified Orsini to manage KEKs). Petitioner's untimely new theories and evidence should not be considered. See Section II.B.2 (citing cases).

Petitioner also argues that a POSITA would be motivated to introduce a KEK into Orsini to further secure the data chunks because “[o]ther references also teach using KEKs to encrypt keys that encrypt ‘partition[s]’ of ‘digital content.’” Reply, 21 (citing new Exhibits 1088, 1080, 1106). But these newly-introduced “other references,” do not form part of Petitioner's combination and should not be considered. See *Edwards Lifesciences Corp. v. Aortic Innovations LLC*, IPR2023-01232, Paper 10, 36 (Feb. 7, 2024) (“Petitioner's rationale to modify [reference] based on inchoate and **unasserted combinations** is also unpersuasive.”); see *Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 886-7 (Fed. Cir. 2024) (“It does not suffice to meet the motivation to combine requirement to recognize that two alternative arrangements ... were both known in the art.”) .

Even if Petitioner's new arguments and evidence were considered, they are meritless. Orsini already teaches “further secur[ing]” the data chunks via a non-cryptographic obfuscation step, and Petitioner fails to explain why a POSITA would be motivated to add a cryptographic step. POR, 21-24. In reply, Petitioner

argues—but fails to prove—that Orsini’s non-cryptographic method is not secure. See Reply, 17, 19, 23-25. Petitioner’s analysis suffers from several critical flaws.

First, Petitioner suggests, citing Dr. Rubin’s testimony, that Orsini’s method of “obfuscat[ing]” share keys is not secure because it does not, “on its own,” provide security. See Reply, 17, 19, 23-25. This testimony is taken out-of-context and does not account for the breadth of Orsini’s methodology and further contradicts Dr. Bhattacharjee’s testimony and Hayhurst. Critically, Orsini’s obfuscation provides security by storing shares in “different locations” from the keys **and** on different “data depositories or storage devices.” Ex. 1005, [0299], [0379]; see Pet., 46. Both experts (and Hayhurst) agree that distributing shares among separate devices results in increased security. Ex. 2046 [Bhattacharjee-2nd-Depo.] 58:23-59:5 (placing shares in separate locations results in “nearly perfect security”); Ex. 1099 [Rubin-Depo.] 130:4-13; Ex. 1007 [Hayhurst] [0008]. And even if a share were recovered, it would be further secured with the other piece of Orsini’s obfuscation step, because an attacker would not be able to decrypt the share with the key stored with it. Ex. 2046 [Bhattacharjee-2nd-Depo.] 46:14-24 (one segment may still have use); 54:10-19 (dataset split into four portions one segment “would have about a quarter of the original data”); 52:15-54:2 (“It’s not clear to me that key 1 would necessarily be useful to decrypt encrypted share 2.”).

Second, Petitioner’s Reply argues that “Orsini’s Figure 21 divides data into four shares/chunks,” and “[t]hat allows (at most) twenty-four different chunk-key pairings,” a number, Petitioner suggests, that could be overcome by a brute force attack. But Orsini’s Figure 21 divides data into “*n*” chunks, *i.e.*, “four ***or more*** shares.” Ex. 1005 [Orsini] [0292]. Petitioner’s scenario, moreover, presumes an attacker acquired ***all*** of the shares comprising the data set. As Dr. Bhattacharjee recognizes, when a file is split into a large number of shares, simply acquiring and reassembling those shares—to say nothing of the additional key obfuscation—would be very difficult, if not impossible given current technology.² Ex. 2046 [Bhattacharjee-2nd-Depo.] 51:24-51:11; Ex. 1007 [Hayhurst] [0008]. It becomes even more difficult when, as Orsini contemplates, the shares are distributed and stored in different physical locations. Ex. 1005, [0292]; *see* Ex. 2046 [Bhattacharjee-2nd-Depo.] 50:24-51:11.

² In deposition, Dr. Bhattacharjee testified—for the first time—that distributing portions of a dataset into shares itself might be cryptographic. Ex. 2046 [Bhattacharjee-2nd-Depo.] 50:5-19. But the step in Orsini’s Figure 21 is not a cryptographic operation as there is no encryption scheme or scrambling/altering of the data. *See* POR, 23; Ex. 2007 [Katz] 4.

Petitioner’s new claim, that a POSITA would be motivated to modify Orsini because its obfuscation method offers “negligible” security is, thus, simply wrong. In any case, Petitioner’s generic appeals to the possibility of increased security is insufficiently generic to establish a motivation. *ActiveVideo Networks, Inc. v. Verizon Commc’ns, Inc.*, 694 F.3d 1312, 1328 (Fed. Cir. 2012) (generic appeals to make a system more efficient or cheaper are “insufficient” to establish a motivation to combine); *Samsung Austin Semiconductor, LLC v. Red Rock Analytics, LLC*, IPR2018-00556, Paper 18, 22 (Aug. 20, 2018) (rejecting “increased utility” as too generic to satisfy motivation).

Moreover, the Reply does not remedy the Petition’s failure to demonstrate that modifying Orsini to “also (or alternatively) encrypt[] Orsini’s share keys using a conventional KEK” would have increased security. Petitioner continues to ignore the POR’s demonstration that adding an additional encryption layer here would likely diminish Orsini’s overall system’s security by adding targets that an attacker could use to compromise the system.³ POR, 25-26; Ex. 2006, 2; Ex. 2008, 1.

³ Dr. Rubin’s testimony regarding increasing security through multiple encryption layers referred to the security of an encryption protocol, not the overall

And Petitioner’s newly proposed modification would do exactly that.

Petitioner’s original modification was to use a KEK with Orsini’s “external **session** key management” which could be modified to “**generat[e]**” the KEK. POR, 27-28; Pet., 25-26. But session key management is very different from KEK management, especially for storage and transport of the keys. POR, 27-28. As the POR demonstrated, the session key management techniques described in Orsini would not adequately protect KEKs. *Id.*

The Reply now argues that “Orsini already taught [other] techniques for managing and securing other KEKs, or (at least) could have been modified ... to use conventional techniques for doing so.” Petitioner, however, does not dispute that the only KEK described in the ’854 is the “workgroup” key not even mentioned in Orsini. POR, 1-6; Ex. 2033 [Rubin-2nd-Decl.] ¶¶37-44. But even if, *arguendo*, Orsini describes KEK management in other embodiments, these techniques are not part of the Figure 21 embodiment, which does not use KEKs. Ex. 1005, [0292]-[0301]. Petitioner fails to explain how or why a POSITA would have been motivated to combine these separate embodiments when Figure 21 already features a non-cryptographic obfuscation step to further secure the shares.

security of a system, contrary to Petitioner’s suggestion. *See* Ex. 2033 [Rubin-2nd-Decl.] ¶¶74-76.

To the extent Petitioner now argues (using new exhibits) that “using/managing KEKs was conventional,” this does not cure Petitioner’s failure to argue that a POSITA would have implemented KEK management in the modification proposed in the Petition. *See* Reply, 26. The mere fact that “managing KEKs w[as] not beyond POSAs’ skill,” even if, *arguendo*, true, does not motivate a POSITA to modify Orsini as proposed, in view of the potential security risks.

Finally, the Reply argues Petitioner’s proposed modification was not driven by hindsight. Reply, 27-28. Petitioner’s proposed modification was hindsight-driven because it followed the ’854’s inventive concept of encrypting share encryption keys with a workgroup key. POR, 29-32 (citing cases). Petitioner’s attempt to introduce new proposed modifications in its Reply to cure the Petition’s inadequate proposal is further indicia that Patent Owner’s hindsight arguments were correct. *See Medtronic, Inc. v. Teleflex Innovations S.A.R.L.*, 70 F.4th 1331, 1347 (Fed. Cir. 2023) (“The Board did not err in discounting modifications not presented in Medtronic’s petition as indicative of hindsight. It was within the Board’s discretion not to consider these untimely raised modifications.”).

IV. CONCLUSION.

The claims should be confirmed.

Respectfully submitted,

/ Stephen J. Elliott /

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

Andrei Iancu (Reg. No. 41,862)

SULLIVAN & CROMWELL LLP

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

Nathan Lowenstein, *pro hac vice*

Colette Woo, *pro hac vice*

LOWENSTEIN & WEATHERWAX LLP

Date: February 3, 2025

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Sur-Reply (the “Sur-Reply”) consists of 5,596 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The Sur-Reply complies with the type-volume limitation of 5,600 words as mandated in 37 C.F.R. § 42.24. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Respectfully submitted,

/ Colette Woo /

Date: February 3, 2025

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served
by electronic service, by agreement between the parties, on the date below:

PATENT OWNER SUR-REPLY

EXHIBIT 2046

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

Elisabeth H. Hunt	EHunt-PTAB@wolfgreenfield.com
Gregory S. Nieberg	GNieberg-PTAB@wolfgreenfield.com
Nathan R. Speed	nspeed@wolfgreenfield.com

Respectfully submitted,

/ Colette Woo /

Date: February 3, 2025