

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case IPR2024-00214
Patent 11,068,609

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

	Page
I. THE BOARD SHOULD DISREGARD THE IMPROPERLY-INCORPORATED REPLY-DECLARATION AND NEW EXHIBITS.....	1
II. THE FOSTER GROUND FAILS (GROUND 2, ALL CLAIMS).....	2
A. “Generating A Plurality Of Data Chunks Based On A Data Set” (Ground 2, All Claims).....	2
B. “Executing Code By A Processor To Perform ... Storing ... At Least One Data Chunk ... On At Least One Storage Device” (Ground 2, All Claims).....	5
C. “Storing, In A Memory Coupled To The Processor, At Least One Data Chunk ... On At Least One Storage Device” (Ground 2, All Claims).	14
1. Anticipation.....	15
2. Obviousness.	16
III. THE ORSINI GROUND FAILS (GROUND 1, ALL CLAIMS).....	21
IV. CONCLUSION.....	29

TABLE OF AUTHORITIES

Page(s)

COURT DECISIONS

<i>Acceleration Bay, LLC v. Activision Blizzard Inc.</i> , 908 F.3d 765 (Fed. Cir. 2018)	9
<i>ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	26
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	8
<i>BlephEx, LLC v. Myco Indus.</i> , 24 F.4th 1391 (Fed. Cir. 2022)	11
<i>Henny Penny Corp. v. Frymaster LLC</i> , 938 F.3d 1324 (Fed. Cir. 2019)	9
<i>In re Kahn</i> , 441 F.3d 977 (Fed. Cir. 2006)	14
<i>In re Magnum Oil Tools Int'l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	14
<i>In re Stepan Co.</i> , 868 F.3d 1342 (Fed. Cir. Aug. 2017)	12
<i>Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	1
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	14
<i>Medtronic, Inc. v. Teleflex Innovations S.A.R.L.</i> , 70 F.4th 1331 (Fed. Cir. 2023)	28

<i>TriVascular, Inc. v. Samuels</i> , 812 F.3d 1056 (Fed. Cir. 2016)	6
<i>Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.</i> , 97 F.4th 882 (Fed. Cir. 2024)	23
<i>Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.</i> , 853 F.3d 1272 (Fed. Cir. 2017)	9
<i>Yita LLC v. MacNeil IP LLC</i> , 69 F.4th 1356 (Fed. Cir. 2023)	9

AGENCY DECISIONS

<i>Cisco Sys., Inc. v. C-Cation Tech., LLC</i> , IPR2014-00454, Paper 12 (Aug. 29, 2014) (informative)	2
<i>Edwards Lifesciences Corp. v. Aortic Innovations LLC</i> , IPR2023-01232, Paper 10 (Feb. 7, 2024)	23
<i>Samsung Austin Semiconductor, LLC v. Red Rock Analytics, LLC</i> , IPR2018-00556, Paper 18 (Aug. 20, 2018)	26

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	Prosecution History of 10,452,854 Patent ['854-FH]
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 (Non-Confidential Redacted Version) (Jan. 8, 2024) [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 Dr. Samrat Bhattacharjee [Bhattacharjee-Depo.]
2035	Reserved
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	Reserved
2040	Reserved
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 in the Petition, it would have hardly needed a **136-page, 26,940-word Reply declaration** and **44 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 Petitioner could now introduce such voluminous new evidence, 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 239 paragraphs. The Reply's *modus operandi* is to include a conclusory sentence purportedly "supported" by citations to up to 16 paragraphs of Dr. Bhattacharjee's reply-declaration. *E.g.*, Reply, 20 (citing ¶¶141-156); 21 (citing ¶¶157-172); 15 (citing ¶¶102-114); 30 (citing ¶¶228-239); 3 (citing

¶¶25-35); 17 (citing ¶¶120-130); 23 (citing ¶¶184-193). The Reply similarly includes unexplained citations to 43 new exhibits. *E.g.*, Reply, 3 (unexplained citations to new exhibits 1073, 1097, 1075-1077, 1092, 1116). This is impermissible incorporation by reference and Petitioner’s 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. THE FOSTER GROUND FAILS (GROUND 2, ALL CLAIMS).

A. “Generating A Plurality Of Data Chunks Based On A Data Set” (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 a data set.” POR, 34-42. The ’609 describes several examples of how to generate shares¹ and makes clear that packets or their payloads are not chunks or shares. *Id.*, 37-39. Indeed, the ’609 identifies a data packet or its packet payload as the dataset to be divided into chunks or shares. *Id.*, 38-39 (discussing Ex. 1001 [’609] 82:15-18, 81:30-31, 81:48-52). The ’609’s usage of

¹ Petitioner does not dispute that the claimed “data chunks” correspond to the “shares” described in the specification. POR, 41-42.

“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.*, 37-38 (citing Exs. 2012-2013, 2036-2038, 2041-2043). The POR further explained that the difference between the ’609’s chunks/shares and Foster’s packets/payloads is significant as the ’609’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.*, 39-40.

In reply, Petitioner does not dispute the ’609’s clear teaching that packets or packet payloads themselves are split into chunks or shares. *See Reply*, 3-5.

Petitioner ignores the patent’s usage and alleges that “SFI suggests a data chunk must be cryptographically split from the data set so the splitting itself makes the data less susceptible to ‘attack.’” *Id.*, 4. But, as seen above, this is not and has never been Patent Owner’s position. Rather, the ’609’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 [’609] 82:15-18, 81:30-31, 81:48-52.

Petitioner argues that the ’609 “places no limit on the relationship between a data set and a data chunk so long as it is a subset of the data set” because “POSAs ‘will recognize ... a wide number of alternatives for the data splitting process.’”

Reply, 4. But Petitioner never argues that or explains why Foster’s MPEG

packetization is a “data splitting process” let alone a suitable “alternative[]” one.

See id. Petitioner contends that “Foster’s payloads ‘are generated to further secure the data’ (POR, 39-40), because Foster encrypts each payload with a different key to ‘provide enhanced security.’” *Id.*, 5. But this misapprehends the purpose of packetization which, as both experts agree, is 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, 5. Indeed, Petitioner argued that Foster’s encryption of the shares teaches “encrypting each respective data chunk of the plurality of data chunks with a respective second key,” rather than “generating a plurality of data chunks based on a data set.” Pet., 65-66, 68-69. Petitioner, thus, fails to rebut the POR’s showing that MPEG packets are not generated to secure data. POR, 39-40.

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, 5. 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 unrebutted.

B. “Executing Code By A Processor To Perform ... Storing ... At Least One Data Chunk ... On At Least One Storage Device” (Ground 2, All Claims).

The POR explained that Petitioner failed to demonstrate that Foster teaches this limitation because Foster’s CPU 406 (the alleged processor) does not execute code to perform storing content units on recipient 430 (containing the alleged storage device). POR, 42-48. Petitioner does not dispute that it did not demonstrate that or explain how Foster’s CPU executes code to store content units on the separate recipient 430, which Petitioner alleged is a “consumer set-top box” in the Petition (Pet., 73). And there is no reason to believe that Foster’s CPU 406 executes any such code as it simply transmits content units to recipient 430 and is agnostic as to what recipient 430 does with the content units after transmission. POR, 42-47; Ex. 2033 [Rubin-2nd-Decl.] ¶¶110-112. Instead, as Petitioner does not dispute, the recipient itself determines whether the content units are stored, and that determination is not based upon any code executed by Foster’s processor. *Id.*

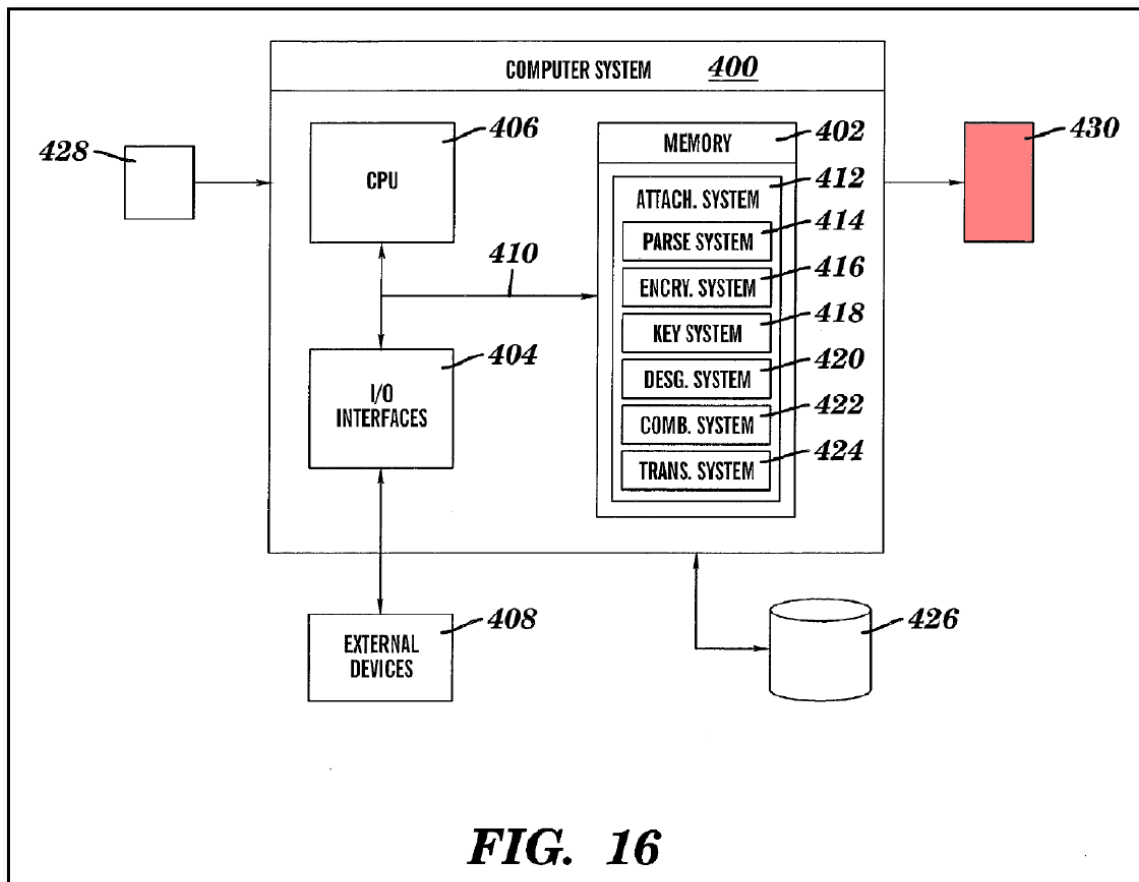
In reply, Petitioner contends that the POR’s showing “is a new construction (EX1060) and SFI identifies no intrinsic evidence requiring the processor to

instruct a storage device.” Reply, 6-7.² But the POR did not offer a new claim construction. Rather, the claim language on-its-face requires that the “processor” “execut[e] code” “**to perform**” storing at least one data chunk on at least one storage device. As the claim says, the processor must execute code that performs storing the data chunks. And, as the POR explained, there is no such code executed on Foster’s processor that “performs” storing at least one data chunk on the recipient or the recipient’s hard drive. POR, 42-47.

Significantly, Petitioner does not identify any code executed by Foster’s processor to perform such storage. Nor does Petitioner dispute that Foster’s system never instructs or sends any instruction to a set-top box to store the content units. See Reply, 6-10.

² Petitioner argues that the “Board properly found that Foster’s processor [executes code that results in storing] because Foster’s methods store encrypted content in memories of storage devices (*e.g.*, on servers and at recipients) coupled to the processor.” Reply, 6 (citing ID, 24-25). But as SFI made no preliminary arguments on whether the processor “execut[es] code” to perform storing, the Board did not make any finding on that limitation. ID, 24-25. Moreover, the Board’s findings at institution are preliminary. *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016).

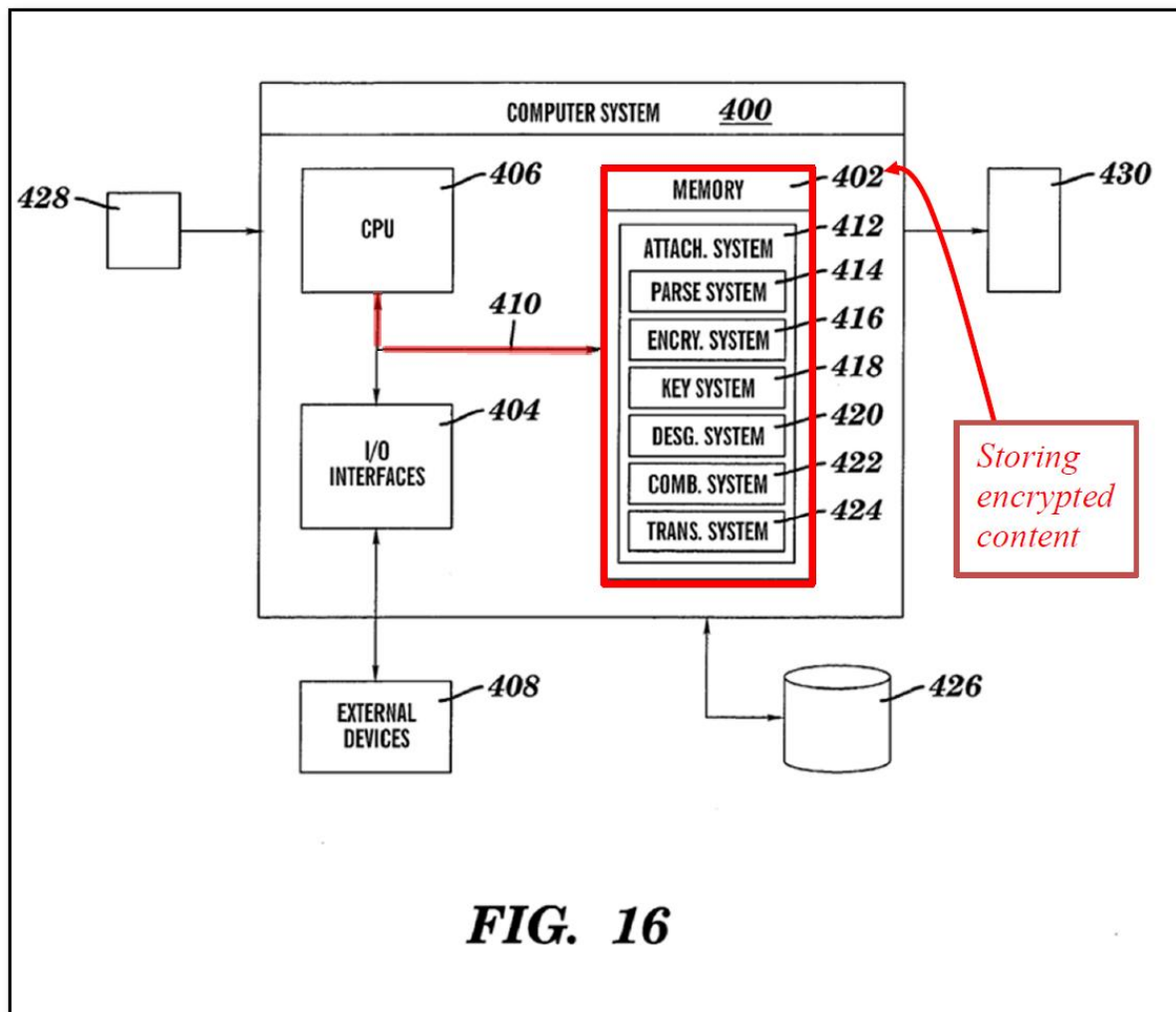
Petitioner further does not dispute that it relied upon a “memory” on a “consumer set-top box” as the alleged “storage device,” as illustrated by the annotated figure in the Petition at 76:



See *id.*; 73, 75 (“Each content unit 116 discussed above is stored on receiver at ‘receipt 430’; **that receiver is a ‘storage device’ (e.g., consumer set-top box)**”).

Implicitly conceding that its original set-top box argument does not anticipate the limitation-in-question, Petitioner does not defend its original theory and instead pivots to new, untimely, arguments. Reply, 6-10. In reply, Petitioner

newly argues that “Foster’s processor executes code that encrypts and stores data on storage-device memory (RAM) directly coupled to it,” relying on Foster’s memory 402:

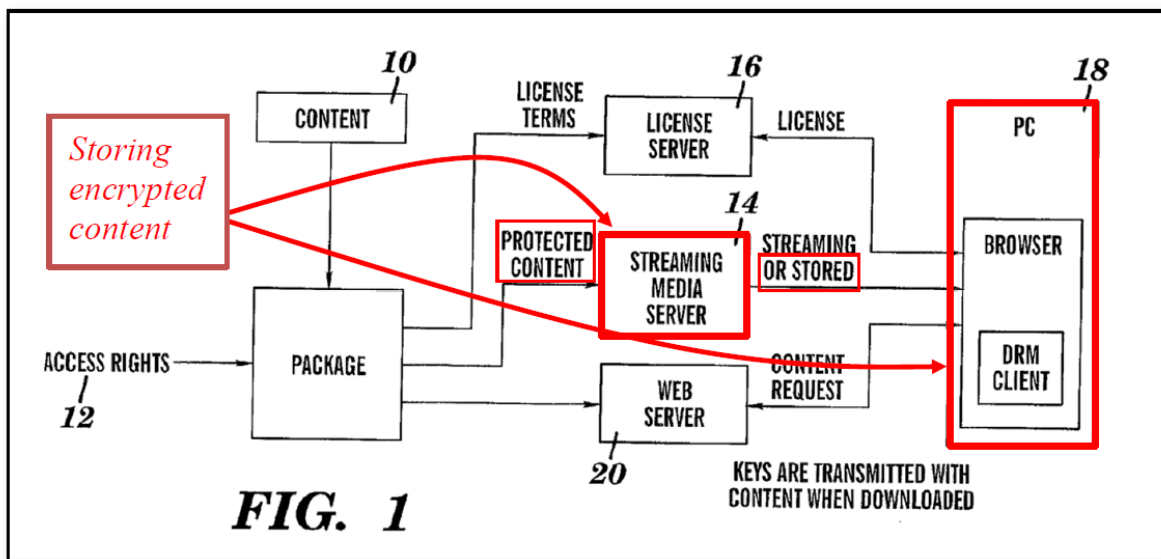


Reply, 7-8. But memory 402 is plainly not the receiver 430 that Petitioner relied upon in the Petition. Consequently, Petitioner should not be permitted to rely upon this new argument. *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1368 (Fed. Cir. 2015) (rejecting shift from “a generic 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.’”) (quoting *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 775 (Fed. Cir. 2018)); *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.”); *Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1286-7 (Fed. Cir. 2017) (“Shifting arguments [in the reply] is foreclosed by statute, our precedent, and Board guidelines.”).

Even if Petitioner’s untimely argument were to be considered, it would still fail. Foster does not disclose storing “content units” (as required by the claims) on “memory 402.” Rather, Foster teaches that “[s]tored in memory 402 is attachment system 412, which includes parsing system 414, encryption system 416, key system 418, designation system 420, combination system 422 and transmission system 424.” Ex. 1006, [0078]. Foster thus teaches that the systems that execute Foster’s methods are stored on memory 402. Foster does not teach that the content units are stored on memory 402. *See id.*

Petitioner also newly relies upon “Foster’s DRMS” and its “media server 14” and “PC 18,” contending that Foster teaches that encrypted content is stored on a media server or personal computer and that Foster’s processor would execute code to perform that storing:



Reply, 9. This argument too is untimely and should not be considered for that reason alone; the Petition never mentions or relies upon this alleged DRMS embodiment. Nor does Petitioner rely upon any “media server” or “personal computer” in the Petition. See Pet., 75.

In addition to being untimely, this new argument is wrong. The “DRMS” described in Foster is Foster’s prior art, not Foster’s inventive system. See Reply, 9; Ex. 1006 [Foster] [0005] (in “Background Art,” “Current technologies ... include a personal computer-based Digital Rights Management System (DRMS)”);

[0049] (“Referring now to FIG. 1, a depiction of a Digital Rights Management System (DRMS) is shown.”), Fig. 1; Ex. 2046 [Bhattacharjee-2nd-Depo.] 24:15-25. Indeed, Foster criticizes the DRMS depicted in Foster’s Figure 1 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”). The DRMS depicted in Figure 1 is, therefore, a prior-art system that Foster’s system is meant to replace and not an embodiment of or foundation for Foster’s inventive system that Petitioner otherwise relies upon.

Thus, whether DRMS allegedly stores content units on a streaming media server or personal computer has no bearing on whether Foster’s system does so. This alone should defeat anticipation as, under such a ground, Foster’s inventive system may not be combined with its admitted prior art. *BlephEx, LLC v. Myco Indus.*, 24 F.4th 1391, 1400 (Fed. Cir. 2022) (“[I]t is not enough that the prior art reference...includes multiple, distinct teachings that the artisan might somehow combine to achieve the claimed invention’ to show anticipation.”) (citations omitted). 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. *In re Stepan Co.*, 868 F.3d 1342, 1346 n.1 (Fed. Cir. Aug. 2017) (when “combining multiple embodiments from a single reference, or selecting from large lists of elements in a single reference, there must be a motivation to make the combination and a reasonable expectation that such a combination would be successful, otherwise a skilled artisan would not arrive at the claimed combination.”).

Finally, Petitioner also argues for the first time in the Reply that Foster teaches a “program stream” for “fixed storage,” such as a “DVD.” As with its other arguments on this point, Petitioner never relied upon a “program stream,” “fixed storage,” or a “DVD” in its Petition. To the extent that Petitioner argues its theory now relies upon a “DVD” as a storage means, Foster does not disclose this. More specifically, Petitioner cannot rely upon a “DVD” as a storage means because a DVD is not a receiver or recipient of content as defined in Foster. *See* Ex. 1006 [Foster] [0040] (“Receiver-a consumer device, such as a set-top box, a DVD **player**, etc., that receives content directly from a content owner, from a content service or from another receiver within a consumer home network.”), [0041] (“Recipient-any entity, such as a content service provider or a receiver, **capable of receiving transmissions.**”).

Petitioner’s new reliance on the “program stream” also fails. As Foster explains, an MPEG stream can be encoded into a program stream or transport

stream, which are each used for different environments. Ex. 1006 [Foster] [0073]. Encoding a stream such that it is optimized for a certain environment, however, is still not the same as the processor executing code *to perform* storing the content units. Encoding a stream of packets does not equate to storing them. Moreover, the “program stream” is irrelevant to Petitioner’s original theory because, as Dr. Bhattacharjee confirms, in the cable environment that set-top boxes are in, a transport stream—which does not require storage of the packets being transported—is used rather than a program stream. 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.

In short, Petitioner’s new contentions that memory 402, streaming media server 14, PC 18, a DVD, or a program stream can replace the “set-top box” that the Petition relied upon as the “storage device” should be rejected as both untimely, and on their merits. Petitioner, thus, again fails to show that Foster discloses the processor executing code to perform storing content units on a storage device.

Petitioner’s obviousness arguments are also deficient. Petitioner disputes that it presented no argument as to how (or why) a POSITA would be motivated to modify CPU 406 to execute code to store encrypted content units on “conventional storage devices,” citing the Petition at 76-78. But this section of the Petition does

not address ***the processor*** executing code at all. See Pet., 76-78 (addressing only how to modify Foster’s memory 402 to store content). Petitioner’s argument that a POSITA “would have known how to implement the feature” because its modification purportedly “relied on conventional storage devices” cannot sustain its argument. Reply, 11-12. As in the Petition, Petitioner’s vague and conclusory argument does not carry Petitioner’s burden. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.”) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *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.”).

C. “Storing, In A Memory Coupled To The Processor, At Least One Data Chunk ... On At Least One Storage Device” (Ground 2, All Claims).

The claims require “storing, in a ***memory coupled to the processor***, at least one data chunk ... on at least one storage device.” Petitioner contends this limitation is anticipated by or obvious in view of Foster. Both arguments fail, as discussed below.

1. Anticipation.

The POR explained that Petitioner failed to show that the alleged “memory” in Foster’s receiver is “coupled to” the alleged processor (the CPU in Foster’s system). POR, 49-51. Because Foster’s processor is agnostic to whether the receiver stores content units, as explained above and in the POR at 42-48, the independent decision at the recipient whether to store the content does not disclose or suggest that any alleged hard drive on the recipient is “coupled to” Foster’s processor. POR, 49-51. Thus, Petitioner has, at most, shown that Foster’s processor is coupled to the recipient, but has failed to show any coupling to the alleged “memory.” *Id.*

In reply, Petitioner does not dispute that the independent decision of whether to store the content units is solely made by Foster’s receiver. Nor does Petitioner dispute that it failed to show how the alleged processor is “coupled to” an alleged memory in the recipient rather than only to the recipient itself (*i.e.*, to its processor). Instead, Petitioner argues that “[t]he Federal Circuit has several times held variants of ‘coupled to’ mean simply ‘connected to.’” Reply, 12 (cleaned up). Petitioner, however, then fails to allege, let alone explain how Foster’s alleged processor is connected to the alleged memory on the alleged storage device. Moreover, Petitioner fails to dispute the POR’s showing that there is no reason to find that the alleged processor is connected to the alleged memory because Foster’s

processor undisputedly has nothing to do with whether content is stored on the alleged memory. *See id.*

As with its argument in regard to the “executing code by a processor to perform storing” limitation, Petitioner again shifts to a new argument. Whereas in the Petition, Petitioner relied upon a memory on a consumer set-top-box, Petitioner’s Reply alternatively invokes Foster’s “local memory,” “media server,” and “DVD drives,” none of which were relied upon in the Petition. *Compare* Pet., 75 (relying upon memory in receiver-STB) *with* Reply 13 (relying on local memory, media server, and DVD drives). Here too, Petitioner’s untimely attempt to change its theory is improper. *See* Section II.B (collecting cases).

Petitioner also argues that the POR “says Petitioner argued Foster’s coupling is only via ‘bus 410,’” and that the POR “ignores transmission system 424, which couples Foster’s processor to storage devices outside Foster’s computer.” Reply, 14-15. This is incorrect. The POR addressed both bus 410 and transmission system 424 and explained how neither provides a communication link to the alleged memory on the alleged storage device. POR, 50-51.

2. Obviousness.

The POR demonstrated that Petitioner failed to show a POSITA would be motivated to modify Foster such that “Foster’s encrypted content [is stored] in the memory of storage devices coupled to the processor (*e.g.*, through a bus, direct

wired/wireless connection, and/or network-based connection).” POR, 52-56 (quoting Pet., 76). The purported benefits Petitioner identified as motivating a POSITA to modify Foster (backup, video-on-demand distribution, and distribution to later-identified recipients) were already solved by Foster’s system because they are provided by the content owner. *Id.*, 52-54. Moreover, there are significant drawbacks to the proposed modifications as they would either compromise security or require significant resources. *Id.*, 54-56. In reply, Petitioner does not dispute that the alleged benefits of the proposed modification are already present in Foster’s system and are provided by the content owner.³

Rather, Petitioner argues that there are benefits of “content-service providers (‘CSPs’)” storing content, and CSPs were known to have stored encrypted content. But Foster’s system is not a CSP. Rather, Foster teaches that a CSP “provides the ‘pipeline’ through which content is delivered from a content owner to a consumer” (Ex. 1006, [0039]) and that the CSP is a “source” of content for Foster’s system which provides encryption and synchronized transmission (*id.*, [0042], [0078]). Thus, Foster’s system receives content **from** a CSP; it is not a CSP storing content. *Id.* That CSPs securely store content does not provide motivation for Foster’s

³ Petitioner calls “content-owner storage” “hypothetical,” but that is precisely what Foster discloses. Ex. 1006 [Foster] [0038], [0042], [0078].

system to store content. And Petitioner’s “corroborating evidence,” old and new, still does not demonstrate that a POSITA would be motivated to modify an intermediary such as Foster’s system, meant only for encryption or securing content, such that it would store the underlying content. As Dr. Rubin testified, using intermediaries allows each to “focus on what they were good at” (Ex. 1099, 93:13-22): intermediary servers can focus on storing content and Foster’s system can focus on encryption and synchronized transmission.

To the extent that Petitioner now argues that Foster’s system would be modified to include a “streaming media server” or “PC,” Petitioner again changes its argument. See Reply, 15-16. In the Petition, Petitioner argued Foster’s memory 402 (in red) would be modified to store encrypted content:

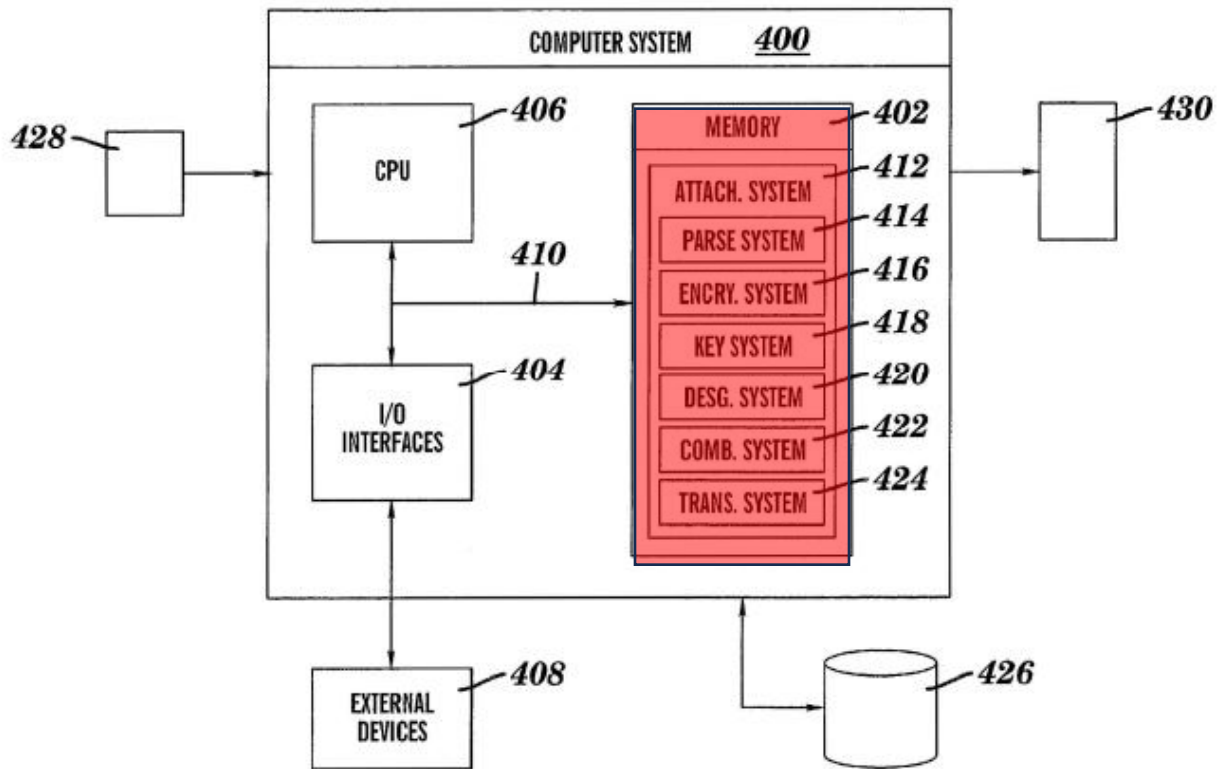
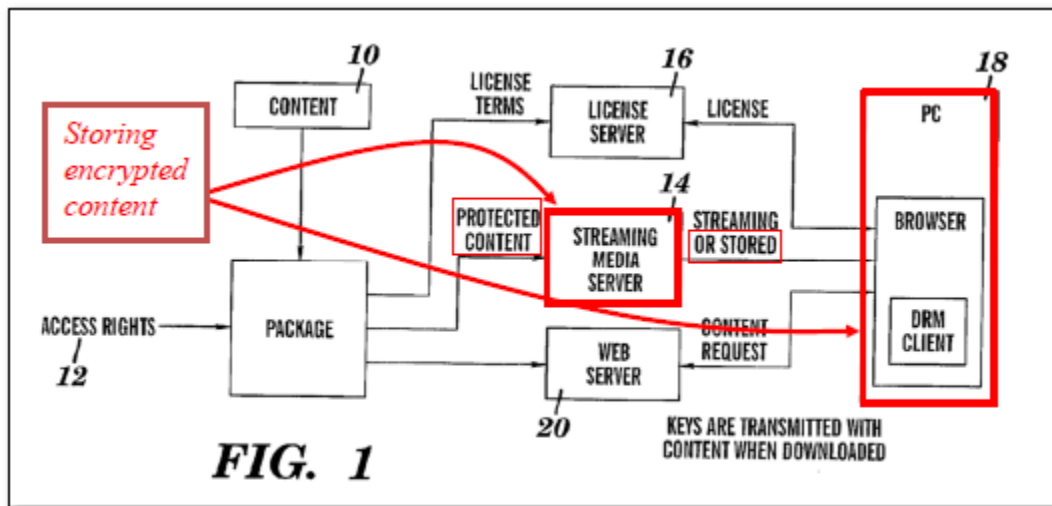


FIG. 16

Pet., 76-77; Ex. 1006, Fig. 16 (annotated). In reply, however, Petitioner argues that Foster's Figure 1 demonstrates that "Foster itself is (at least) suggesting/motivating having its processor execute code for storing on storage devices *coupled to* Foster's processor, to support content-on-demand (like VOD) and/or backup":



Reply, 15-16. As explained above, Petitioner never relied upon Figure 1’s prior-art DRMS and does not explain why a POSITA would be motivated to combine Foster’s prior-art with Foster’s inventive system, especially in light of Foster’s criticism of DRMS. See Section II.B; Ex. 1006 [Foster] [0051].

Finally, Petitioner does not dispute that Foster’s system would have required significant modifications to prevent compromising security and significantly more storage. See Reply, 17-18. Petitioner argues that “content owners often had intermediaries storing their content.” But that is simply irrelevant to the question of whether Foster’s system—which only encrypts content and then immediately transmits it—would have sufficient security for long-term content storage.

Petitioner argues that “Foster’s encryption adds security.” Reply, 18. But Foster’s system adds encryption to content that is immediately transmitted, and it is not designed for long-term secure storage of the underlying content. See Ex. 2046

[Bhattacharjee-2nd-Depo.] 58:12-59:15 (there is a distinction between cryptography and security). The Petition merely proposed modifying “memory 402” to also store encrypted content without addressing how the newly stored content would be secure. Pet., 76. And while Petitioner argues that “content owners often had intermediaries storing their content,” Petitioner does not argue that Foster would be modified to add the security from these intermediaries. Encrypting content but leaving it in unsecured storage would, in fact, compromise security. POR, 54-55; Ex. 2033 [Rubin-2nd-Decl.] ¶126.

III. THE ORSINI GROUND 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, 35-51. Rather than defend its positions, Petitioner abandons everything but “one obviousness argument.” Reply, 19. 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 share keys with a KEK allegedly found in another Orsini embodiment. Reply, 19; Pet., 40-42. The Board, however, has already found that Petitioner failed to sufficiently demonstrate this theory in

the Petition. ID, 50-51 (“Petitioner does not provide a sufficient rationale for combining these multiple embodiments.”).⁴

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.*, 20-23. 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.*, 23-27. As the Board found, Petitioner’s arguments were driven by hindsight. *Id.*, 27-32.

Instead, Petitioner’s Reply introduces new theories and untimely evidence to attempt to fill the Petition’s holes. *E.g.*, Reply, 27-28 (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*

⁴ Undisputedly, “performing a cryptographic operation based on the first 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, 18-20.

Section II.B (citing cases). Petitioner’s need to rely on untimely theories and new purported evidence only underscores that its Petition failed to establish that the claims are invalid.

Petitioner also argues that a POSITA would be motivated to introduce a KEK into Orsini to further secure the data chunks because “[o]ther prior art similarly teach using a KEK to encrypt keys, including keys that (like Orsini) encrypt ‘partition[s]’ of data.” Reply, 23 (citing new Exhibits 1088, 1080). 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, 20-23. In reply, Petitioner

argues—but fails to prove—that Orsini’s non-cryptographic method is not secure. See Reply, 20, 22, 26-28. 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, 20, 22, 26-28. 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., 43-44. Both experts (and the Hayhurst reference asserted in the related IPR2024-00215) 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; *e.g.*, Ex. 1116 [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 (if dataset is 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 share-key pairings,” a number, Petitioner suggests, that could be overcome by a brute force attack. Reply, 25. But Orsini’s Figure 21 divides data into “*n*” chunks, which is “four ***or more*** shares.” Ex. 1005 [Orsini] [0292]. Petitioner’s scenario, moreover, presumes that an attacker could acquire ***all*** of the shares that comprise 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 determining which key decrypts which share—would be very difficult, if not impossible given current technology.⁵ Ex. 2046 [Bhattacharjee-2nd-Depo.] 51:24-51:11; *see also* Ex. 1116 [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.

⁵ 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, 21-22; 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 insufficient, as a matter of law, 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 nothing to remedy the Petition’s failure to demonstrate that modifying Orsini to “also (or alternatively) encrypt[] Orsini’s share keys using a conventional KEK” (Reply, 25) 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.⁶ POR, 24-25; Ex. 2006, 2; Ex. 2008, 1.

⁶ 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, decreasing the security of the system as a whole. Petitioner’s original modification was to use a KEK with Orsini’s “*session* key management” which could be modified to “*generat[e]*” the KEK. POR, 25-27; Pet., 23-24. But session key management is very different from KEK management, especially for storage and transport of the keys. POR, 25-27. 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 managing KEKs.” Reply, 27. Petitioner, however, does not dispute that the only KEK described in the ’609 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

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

embodiments when Figure 21 already features a non-cryptographic obfuscation step to further secure the shares. 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, 27. 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, 29-30. Petitioner’s proposed modification was hindsight-driven because it followed the ’609’s inventive concept of encrypting share encryption keys with a workgroup key. POR, 30-32 (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.

Petitioner fails to demonstrate by a preponderance of the evidence that any of the claims are invalid.

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 5,476 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