

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case IPR2024-00212
Patent 11,178,116

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 PETITION’S TAJIMA GROUNDS FAIL (GROUNDS 1-4).....	2
A. Tajima-Foster Fails (Ground 2, Claims 1-2, 9, 11-14)	2
1. Foster Confronts a Different Problem in a Different Field than Tajima	2
2. Applying Foster’s KEK Technique to Tajima Would Be Redundant	6
B. Tajima-Rivest Fails (Ground 3, Claims 9-14)	9
C. Tajima-Rivest-Shyu Fails (Ground 4, Claims 1-3, 6).....	11
D. Tajima Alone Fails (Ground 1, Claims 1, 5-8)	13
III. FOSTER-HAYHURST FAILS (GROUND 5, CLAIMS 1-2, 5, 9, 11) ..	14
A. Petitioner Fails to Prove Hayhurst Is Analogous Art.....	14
B. The Petition Fails to Demonstrate a Motivation to Combine Foster and Hayhurst	17
1. Petitioner Does Not Dispute that Foster-Hayhurst Would Thwart Foster’s Fundamental Aims	17
2. Petitioner Improperly Changed Its Unpatentability Theory	20
3. Petitioner’s New Theories Are Meritless.....	23
IV. CONCLUSION	26

TABLE OF AUTHORITIES**Page(s)****CASES**

<i>Arbutus Biopharma Corp. v. ModernaTX, Inc.</i> , 65 F.4th 656 (Fed. Cir. 2023)	13
<i>Arctic Cat Inc. v. Polaris Indus.</i> , 795 Fed. App'x 827 (Fed. Cir. 2019)	20
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	22
<i>Cisco Sys., Inc. v. C-Cation Tech., LLC</i> , IPR2014-00454, Paper 12, 9-10 (Aug. 29, 2014).....	2
<i>Donner Tech., LLC v. Pro Stage Gear, LLC</i> , 979 F.3d 1353 (Fed. Cir. 2020)	16
<i>Henny Penny Corp. v. Frymaster LLC</i> , 938 F.3d 1324 (Fed. Cir. 2019)	22
<i>HTC Corp. v. Cellular Commc'ns Equip. LLC</i> , 877 F.3d 1361 (Fed. Cir. 2017)	13
<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 US 398 (2007).....	5
<i>Netflix, Inc. v. DivX, LLC</i> , 84 F.4th 1371 (Fed. Cir. 2023)	25
<i>Unigene Labs., Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	4
<i>Yita LLC v. MacNeil IP LLC</i> , 69 F.4th 1356 (Fed. Cir. 2023)	22

REGULATIONS

37 C.F.R. §42.6(a)(3) 2

OTHER AUTHORITIES

Consolidated Trial Practice Guide 1

EXHIBIT LIST	
2001	Reserved
2002	Reserved
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 (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) [Cambridge-Dictionary]

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	Excerpts from Oxford University Press, <i>Oxford English Dictionary</i> (12th ed. 2012) [Oxford-English-Dictionary]
2024	Excerpts from HarperCollins Publishers, <i>English Dictionary for Advanced Learners</i> (3d ed. 2001) [Collins-Dictionary]
2025	Japanese Patent Application Publication No. JP2003046500A to Tajima <i>et al.</i> [Tajima-Japan-Application]
2026	Cambridge Dictionary, 登録, https://dictionary.cambridge.org/us/dictionary/japanese-english/%E7%99%BB%E9%8C%B2 (last visited Mar. 22, 2024) [Cambridge-Japanese-English-Dictionary]
2027	TechTarget, <i>Certificate Authority</i> , https://www.techtarget.com/searchsecurity/definition/certificate-authority (last updated Sept. 2021) [TechTarget]
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	Cambridge Dictionary, 登録, https://dictionary.cambridge.org/us/dictionary/japanese-english/%E7%99%BB%E9%8C%B2 (last visited June 17, 2024) [SERVED, NOT FILED]
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, PhD.
2034	Deposition Transcript of Dr. Samrat Bhattacharjee, taken on August 9, 2024 [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]
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]
2042-2044	Reserved
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-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016). Had Petitioner done so, it would not need a **118-page, 25,000-word Reply declaration, comprising 201 paragraphs of additional testimony** and **42 new exhibits** to respond to the POR. 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 introduce such voluminous new evidence, unexplained citations to its new reply-declaration in its Reply constitute improper incorporation by reference (Section I) and fail to demonstrate 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 new exhibits are improperly incorporated by reference and should be disregarded. The Reply does not meaningfully discuss most of the reply-declaration’s 201 paragraphs. Instead, it typically includes a conclusory sentence purportedly “supported” by citations of up to a dozen (or more) paragraphs of Dr. Bhattacharjee’s reply-declaration. *E.g.*, Reply, 22 (citing ¶¶65-80); 26 (citing ¶¶128-142); 27 (citing ¶¶145-58). The Reply similarly

includes unexplained citations to 42 new exhibits. *E.g.*, Reply, 26 (unexplained citations to new exhibits 1073, 1097, 1075, 1076, and 1077). This impermissible incorporation by reference and unexplained citations 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 PETITION’S TAJIMA GROUNDS FAIL (GROUNDS 1-4).

A. Tajima-Foster Fails (Ground 2, Claims 1-2, 9, 11-14).

1. Foster Confronts a Different Problem in a Different Field than Tajima.

In its Reply, Petitioner asserts that a POSITA would be motivated to combine Foster with Tajima, arguing that both are in the same field because Foster purportedly “relates to ‘security of content’” while Tajima “improves the security of personal information.” *See* Reply, 13 (citing EX1005 [Tajima], [0044]; EX1006 [Foster], [0003]). This is incorrect and Petitioner’s argument obscures the substantial differences between the fields of these two references and the problems they address.

Tajima is directed to long-term “registration” (*e.g.*, storage) of personal information in areas connected to the Internet, particularly in the e-commerce context. EX1005 [Tajima], [0044]; EX2046 [Bhattacharjee-2nd-Depo.], 81:9-10 (“The Tajima I know discusses shopping.”). It discloses a system and method for securing personal shopping information by dividing the personal information into

“data portions” or “data fragments” and storing each fragment in a different location, where each location is under “separate” control. EX1005 [Tajima], [0046]; *see, e.g.*, POR, 23-24. When the data portions are encrypted, Tajima stores information regarding the encryption key used to encrypt one data fragment with a different fragment that the key cannot decrypt. This means that a data portion and information regarding the key that can decrypt it are stored in different locations controlled by different entities. *Id.*

Foster, in contrast, is focused on data transmission, more specifically, “synchronized” transmission of a media content packet with the key (also encrypted) used to encrypt the packet in “a single stream” to a single recipient, *i.e.*, a set-top box. *See, e.g.*, EX1006 [Foster], [0009]; POR, 13-16. Foster, directly contrary to Tajima, assumes the data will be provided in a continuous stream of packets, all going to the same location, and therefore relies on encryption to protect each packet.

In Foster’s invention, unlike Tajima’s, each packet *must* be kept with the “title” key that can be used to decrypt it. EX1006 [Foster], [0009]. As Foster explains, “under the present invention” a “title key used to encrypt content is itself encrypted with a key encryption key and attached to the encrypted content for synchronized transmission to a recipient.”

Thus, as the POR showed, in the normal course of research and development, a POSITA would not have naturally combined these references, from different fields, that are fundamentally at odds, and that are directed toward solving fundamentally different problems. POR, 16 (citing EX2033 [Rubin Decl.], ¶62); *see also Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011).

In its Reply, Petitioner argues that both are in the same field because Foster purportedly “relates to ‘security of content [data]’” while Tajima “improve[s] the security of personal information.” *See* Reply, 13 (citing EX1005 [Tajima], [0044] and EX1006 [Foster], [0003]).¹ This is incorrect; Tajima relates methods and systems for improving the security of personal information in the on-line shopping context, while Foster addresses media content but does not purport to improve the security of such content as compared to the prior art. Foster teaches, not improved data security, but rather a way of avoiding the “inherent latencies (*e.g.* delays)” in providing random access to content associated with prior art systems that lacked synchronized transmission of keys and content in the streaming context. EX1006 [Foster], [0063], Fig. 8; POR, 13-15.

Petitioner also argues that, even if they are in different fields, a POSITA would simply have plucked a single feature of Foster—its “teaching to use a KEK

¹ Contrary to Petitioner’s claim, Paragraph [0003] of Foster says nothing about “security of content.”

to encrypt keys”—and applied it to Tajima, ignoring its other, contrary teaching that the KEK must be kept with the packet, which would have discouraged such application. Reply, 13. Petitioner thus relies on hindsight, not a showing of obviousness. “If a technique has been used [in a reference] to improve one device,” it can be combined with another only if “a [POSITA] would recognize that it would improve similar devices in the same way.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 401 (2007).

Here, a POSITA would not recognize that the KEK technique of Foster could be used to improve Tajima, much less to improve it “in the same way.” Foster’s KEK technique does not improve data security as compared to the prior art, which also used encrypted packets. See EX1006 [Foster], [0004]-[0005]; POR, 12-13. Foster’s technique simply allows synchronous transmission of a key with the content it can decrypt, in order to reduce the delays associated with prior art media technologies. EX1006 [Foster], [0063]. Such delays are not present, and need not be avoided, in Tajima.

In fact, Foster discourages the use of its KEK technique with Tajima, by stressing the importance of keeping the title key with the content it encrypts. POR, 27. The only reason for using the KEK in Foster is **because** the title key is kept with the content it decrypts; the KEK provides security because it prevents someone with access to all of the content from decrypting it. See POR, 15-16;

EX2034 [Bhattacharjee-Depo.], 32:20-23 (“synchronous transmission of [of key and content] was “the whole invention” of Foster). In direct contrast to this teaching of Foster, Tajima stores each data portion with information regarding a key that cannot decrypt it in a different, separately controlled location. Tajima thus confronts a different problem than Foster’s problem because it is unlikely that a single attacker could gain access to all of the portions in separately controlled locations. EX2046 [Bhattacharjee-2nd-Depo.], 58:23-59:5 (removing part of a data set from its “original computer” and storing it in another separate location (*e.g.*, on a USB drive) provides “nearly perfect security.”); *see also infra* at 6-8. The reason Foster uses its KEK technique is simply absent from Tajima and a POSITA would not have considered combining them in the normal course of research and development. *See* POR, 26-27.

2. Applying Foster’s KEK Technique to Tajima Would Be Redundant.

In the POR, Patent Owner showed that a POSITA would not have been motivated to combine Foster with Tajima because doing so would render Tajima’s method of securing the keys used to encrypt its data portions redundant. POR, 23-25. Petitioner’s Reply argues that using Foster’s KEK technique in Tajima would not be redundant, simply because it would “provide[] more security.” Reply, 16. Petitioner acknowledges that Tajima does not suggest any need for

Foster's technique or for improved security, but identifies one situation in which it contends this might arise: "[A]n attacker able to recover all of Tajimas' data fragments will possess all of the plaintext keys used to encrypt the entire data set" and thus would be able to decrypt it. Reply, 17 (ellipses omitted).

Adding key encryption to Tajima is redundant because Tajima's invention is expressly designed to address the issue Petitioner identified. Tajima acknowledged that, in prior art systems, data portions might be insecure in the those circumstances. Tajima notes that:

[if all of the data portions are] registered with one area as a contiguous data file, this information may be viewed by unauthorized access from the outside through a security hole or by unauthorized access by someone inside the system.

EX1005 [Tajima], [0042]. But Tajima also points out that in these circumstances encryption does not provide the necessary security because:

a method can be employed in which [] information is registered with an encrypted state...[but] the danger still remains that...given enough time, a high-speed computer may be used to decrypt [the information].

Id., [0043].

Tajima addresses the problem that an attacker might acquire all of the data portions (and thus the information regarding the keys necessary to decrypt them)

by storing each data portion in a different, separately controlled location. This is critical to Tajima's invention. As Tajima explains, in "the present invention":

because personal information that is registered with areas that are connectible to the Internet is divided into a plurality of data portions and then registered with areas that are each under separate control, the personal information cannot be viewed unless all of the areas in which data are registered are exposed, and an improvement can therefore be obtained in the security of personal information that is registered with areas that are connectible to the Internet.

EX1005 [Tajima], [0048]. Tajima recognized that storing the information in different, separately controlled locations meant that an attacker would be very unlikely to get access to every portion of the personal information because it is unlikely the same security flaw would exist at two locations separately controlled by different entities, or that an insider at one location could get access to a data portion stored in a database controlled by another entity. *See id.*, [0044]-[0046] (describing the improvement). As Petitioner's expert, Dr. Bhattacharjee, explained at his deposition:

The idea is that if data is stored in different places, then ideally, if one site compromised, that does not automatically, you know, lead to a compromise at another site. One way to potentially decrease that chance is to make them have different control. Potentially they will use

different methods, different security protocols and that could reduce the chance of one compromise spilling over to another.

EX2046 [Bhattacharjee-2nd-Depo.], 91:20-92:3; *see also id.*, 58:23-59:5.

Thus Tajima's system offers greater security over systems that use key encryption, to avoid the only situation Petitioner has identified in which it claims Foster's KEK technique might "provide more security." Tajima discloses an improvement specifically to overcome that problem, by preventing an attacker from obtaining all of the data portions. To add another layer of KEK encryption on top of Tajima's invention, when Tajima avoids the need for KEKs, is the very definition of a "redundant" combination.

B. Tajima-Rivest Fails (Ground 3, Claims 9-14).

In the POR, Patent Owner showed that a POSITA would not combine Tajima with Rivest's all-or-nothing transformation ("AoNT"), because standing alone Rivest does not provide additional security; for this reason, Rivest is generally used in combination with further encryption techniques that require a secret key. POR, 28-29. In its Reply, Petitioner contends that Rivest could provide security by carrying out the AoNT with a public key like that in Tajima, arguing that an attacker would not know "that AoNT was applied in the first place" or "that a user's public key, and which user's public key, was used." Reply, 19.

Rivest does not mention public keys and is not intended to be used with public key encryption as proposed in the Petition. POR, 28-29. Petitioner does not dispute this. In addition, by basing security on maintaining the secret of the algorithm and using a key that is publicly available, Petitioner's proposed combination would violate the most fundamental rule of cryptography, Kerckhoff's principle. This requires that "a cryptosystem should be secure even if everything about the system, except the key, is public knowledge." See POR, 33; EX2033 [Rubin Decl.], ¶94; EX2007, 3.

In Petitioner's proposed combination, the opposite is true: The key is public knowledge, but use of AoNT is purportedly kept secret. But Rivest's transformation algorithm is known from Rivest itself, and there are only a limited number of algorithms that might be used; an attacker could simply try them all. *Id.* Public keys are, by definition, public, accompanied by certificates that identify the key's holder. EX1005 [Tajima], [0075]. A POSITA would recognize that the combination of Tajima and Rivest, as proposed in the Petition and explained in the Reply, could not provide any reliable security based on the use of a secret algorithm and a public key.

The POR also showed that a POSITA would not be motivated to combine Tajima with Rivest because Rivest discloses that its transformation has "terrible error propagation properties." POR, 31. Petitioner's Reply suggests, without

explanation, that “Tajima-Rivest avoids...error propagation because individual transformed message blocks are kept and transmitted together.” Reply, 20.

However, Rivest explains that any transmission of the transformed data that results in damage to a data fragment, even the loss of a single bit, can prevent inversion of the transformation. Rivest teaches that, when its AoNT is used:

If any ciphertext block is damaged, then it is likely that *every* message block will be damaged. Thus, ciphertext should be transported with reliable transmission means.

EX1034, 216. Petitioner admits that in its proposed combination, “individual transformed message blocks are kept ***and transmitted*** together,” Reply, 20, the same action that Rivest discloses can lead to damage that would prevent inversion of the transformation. Thus Petitioner’s Tajima-Rivest would require additional, failure-proof error-correction techniques not disclosed in either Tajima nor Rivest.

C. Tajima-Rivest-Shyu Fails (Ground 4, Claims 1-3, 6).

The POR showed that a POSITA would not be motivated to combine Tajima-Rivest-Shyu because Shyu violates Kerckhoff’s principle by proposing to achieve security through concealing the encryption (“scrambling”) algorithm used on a data set or piece of a data set. POR, 32-34. Petitioner’s Reply argues that Shyu does not violate Kerckhoff’s principle because “Shyu does not use secret algorithms,” but rather “selects from among known algorithms.” Reply, 20.

Contrary to Petitioner’s argument, Shyu makes clear that whatever security it may provide *is* due to the secrecy of its algorithms. Shyu teaches that the use of a single algorithm may be inadequate to prevent software piracy because “the protection...is weak once the scrambling algorithm has been broken by hackers.” EX1016 [Shyu], 1:27-29. A system in which the algorithms must be “broken” by an attacker is a system that uses secret algorithms. Shyu’s purports to solve the problem through a system “wherein the scrambling algorithm [is] dynamically changed” to use different undisclosed algorithms on different pieces of a data set that is to be transmitted. *Id.*, 1:35-42.

The POR also showed that Shyu’s focus on data transmission to a single source, in contrast to Tajima’s focus on data storage in multiple locations, would discourage a POSITA from combining the two references. POR 34-35; *see also* Reply 21. Petitioner argues its “Tajima-Rivest-Shyu combination applies Shyu’s principle to increase security of Tajima’s data fragments after storing, not during transmission.” Reply, 21. But as Patent Owner explained in the POR, Shyu purports to prevent software piracy during software transmission where a single attacker would have access to every piece of the data set. POR, 34. Shyu’s technique would be irrelevant and redundant to Tajima, which prevents an attacker from getting access to every piece by storing the pieces in different, separately controlled locations. *See supra* at 6-8; POR, 34.

D. Tajima Alone Fails (Ground 1, Claims 1, 5-8).

In Ground 1, the Petition contends that Tajima anticipates or renders obvious independent claim 5 and dependent claims 5-8 of the '116. Claim 5 requires “storing each data chunk...together with one of the plurality of obfuscated different encryption keys.” The Petition fails to show that Tajima discloses or suggests this limitation because Tajima stores “information regarding the key” with the data fragments, but does not disclose or suggest that the key itself is encompassed by “information regarding the key.” POR, 1-8.

In its Reply, Petitioner argues that, for purposes of anticipation, Tajima actually discloses that “information regarding the key” includes the key itself, relying on what a POSITA would have “understood” from inferences purports to draw from other disclosures Tajima. Reply, 2-7. This argument fails because the Federal Circuit has repeatedly explained that “[t]o anticipate a claim, a single prior art reference must disclose every limitation of the claimed invention either expressly or inherently.” *HTC Corp. v. Cellular Commc’ns Equip. LLC*, 877 F.3d 1361, 1368-69 (Fed. Cir. 2017); *see also Arbutus Biopharma Corp. v. ModernaTX, Inc.*, 65 F.4th 656, 661-65 (Fed. Cir. 2023).² It is undisputed that, in the

² Petitioner disputes the requirements for anticipation, relying on a 57-year-old case and a 20-year-old case that generally describe the same requirements using somewhat different language. *See* Reply, 2.

embodiments on which the Petition relies, Tajima does not expressly state that the key itself is attached to data fragments. Thus, Petitioner is necessarily relying on an inherent disclosure, but cannot dispute that the Petition does not make the required showing. Reply, 2; POR, 2-3.

Petitioner also argues that modifying Tajima's key information to include the key itself would have been "obvious" and "conventional." Reply, 8-9. As to conventionality, Petitioner relies on prior work by three of the '116 Patent's inventors that it did not include as a ground for invalidity in the Petition. *See* Reply, 9-10. As to obviousness, the POR showed that the Petition could not rely on "common sense" to supply a limitation that Tajima did not itself disclose. POR, 5-6. Petitioner's Reply now disclaims reliance on common sense, and contends it relied on "reasoned analysis," but they amount to the same thing: its expert's same unfounded inferences and speculations already addressed in the POR. *See* Reply, 8-11; POR, 4-8.

III. FOSTER-HAYHURST FAILS (GROUND 5, CLAIMS 1-2, 5, 9, 11).

A. Petitioner Fails to Prove Hayhurst Is Analogous Art.

Petitioner has the burden of proving Hayhurst is analogous art and did meet that burden in the Petition. POR, 38-47. The Reply fares no better. To meet its burden, Petitioner was required to identify the field of endeavor to which the '116 relates, and the problem(s) that Hayhurst attempted to solve. POR, 38-39 (citing

cases). Petitioner declined to do either. Reply, 21-24; EX1111 [Bhattacharjee-2nd-Decl.] ¶63 (“I have not been asked to opine on whether SFI has identified the correct field of endeavor for the ’116 patent.”); *see also* Reply, 5-6 (not identifying problem Hayhurst sought to address); EX1111 [Bhattacharjee-2nd-Decl.] ¶¶27-47 (same). Thus, the Reply cannot rectify Petitioner’s failure to carry its burden.

The ’116 and Hayhurst do not share the same field. POR, 39-43; EX2033 [Rubin-2nd-Decl.] ¶¶108-110. The ’116’s field is securing data, while Hayhurst’s field is decentralized media delivery. The Reply does not dispute the ’116’s field but attempts to identify Hayhurst’s field by its reference to “secure handling and storage.” Reply, 21 (discussing EX1007, [0002]). Petitioner ignores the immediately preceding clause, which states: “[t]his application relates to ***the field of electronic media delivery, such as video-on-demand***[.]” EX1007, [0002].

Petitioner similarly ignores that each of Hayhurst’s title, abstract, technical field, background, summary, specification/figures, and claims—traditionally used to discern the field of endeavor—***all*** confirm that Hayhurst’s field is “decentralized media delivery.” *See* POR, 41-43.

Petitioner instead asserts that that “decentralized media delivery” not Hayhurst’s field, but merely “is how Hayhurst provides ‘security,’” Reply, 21, and “deterrence to piracy.” Reply, 31. But this gets Hayhurst backwards; security and deterrence to piracy is a by-product of its decentralized media delivery, which

seeks to overcome bandwidth inefficiencies associated with prior art video-on-demand systems. EX1007 [Hayhurst] [0004]-[0006]. Solely as a by-product, Hayhurst suggests, 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, 41-42 (discussing EX1007 [Hayhurst], Title, Abstract, [0002], [0003]-[0004], [0005], [0012], [0015]).

As for the reasonable pertinence prong of the analogous art test, “***the problems to which both [the claimed invention and the reference] 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 identifies the problem Hayhurst sought to solve or compares it to the problem solved by the ’116.

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.” EX1007, [0004]-[0005]; POR, 45-46; EX2033 [Rubin-2nd-Decl.] ¶113. Petitioner does not dispute that Hayhurst’s limited bandwidth problem is not reasonably pertinent to the ’116’s problem of eliminating user-related vulnerabilities in storing sensitive

information or any other “additional” problems Petitioner suggests the ’116 addresses. POR, 47; EX2033 [Rubin-2nd-Decl.], ¶¶117-116; Reply, 22-24.

B. The Petition Fails to Demonstrate a Motivation to Combine Foster and Hayhurst.

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, 55 (citing Pet., 67, 63). Petitioner’s combination applied Hayhurst’s storage techniques to all of “Foster’s encrypted content units.” POR, 58-59 (citing Pet., 61-64; EX2034 [Bhattacharjee-Depo.], 126:3-9).

The POR explained that the proposed Foster-Hayhurst combination would undermine Foster’s fundamental aims. POR, 57-68. 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.*, 58-64.

Foster’s emphasis is avoiding delays to allow 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 “foster random access to content”

at a (single) receiver was “sort of the whole invention in Foster.” EX2034 [Bhattacharjee-Depo.], 32:20-23. The Foster-Hayhurst combination, however, would thwart these aims because 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.*, 57-64. The synchronization of keys and content required by Foster is irrelevant to Hayhurst. *Id.*, 57-58.

In its Reply, Petitioner argues that Foster is not “limited to streaming ‘live’ broadcasts” and “also concerns storing secured data.” Reply, 26-27. But Patent Owner has never argued that Foster is so limited. 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. POR, 12-13; *see also* EX1006 [Foster], [0006]-[0007], [0050], [0052].

Foster-Hayhurst should also 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, 64-67. In its 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, 27-28. This is 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.***” EX1006 [Foster], [0054]; see EX2046 [Bhattacharjee-2nd-Depo.], 25:21-27:10 (“reencrypting a content would be more time-consuming than reencrypting a key.”).

Petitioner argues, without explanation, that “POSAs also knew how to change/replace KEKs across many devices/users.” Reply, 28 (citing new Exhibits 1078-1080). But aside from being untimely, none of its newly cited exhibits involve changing/replacing KEKs, much less across many devices/users. See EX1078, 4:5-28 (concerning information delivery method in peer-to-peer network, not KEKs); EX1079, 544-546 (replacing session keys, not KEKs); EX1080, 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, 64-67. In reply, Petitioner argues for the first time that “Foster-Hayhurst does not distribute the KEK to user devices” because “[a]s in Foster alone, Foster-Hayhurst would only give access to a KEK once authorized to decrypt the content.” Reply, 28 (citing EX1006, [0049],

[0052]). Petitioner, however, relies on Foster’s description of prior art, rather than Foster’s system. EX1006 [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, 65-67. Thus, rather than having only one copy of a KEK exposed, as many KEK copies are exposed as there are reassembled content files. *Id.*

Ultimately, “[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 56-57, 35 (citing additional cases). But Petitioner 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, 24-29.

2. Petitioner Improperly Changes Its Unpatentability Theory.

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, 24.

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” and never mentions it. The Reply wrongly asserts that Foster’s storage context was “relied upon in the Petition,” citing the Petition at “51-53.” *See* Reply, 24. But these pages do not evidence any reliance upon Foster’s “storage context” for the Foster-Hayhurst combination; they do not even mention Hayhurst. *See* Pet., 51-53.

Rather, the Petition argued that “the Foster-**Hayhurst** combination” allegedly uses “Foster’s technique of securing a data set,” not **storing** such content. *Id.*, 64. The Petition expressly relied upon “**Hayhurst’s technique of storing** encrypted media segments in a distributed manner across a network of subscriber devices” and on “**Hayhurst’s technique of redundantly storing media segments on the subscriber units.**” *Id.* The Petition at 66 argued that in the **Foster-Hayhurst** combination, the content provider “distributes the processed content units 116 to different respective Foster-Hayhurst subscriber units” so that each “is redundantly **stored as taught by**

Hayhurst.” In short, the Petition’s Foster-Hayhurst combination relied on Hayhurst’s storage methods, not Foster’s.

Petitioner’s improper shifting of its unpatentability theory to rely on Foster’s “storage context” demonstrates 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 [the reference] that any [] method can be used” to reliance upon “previously unidentified [specific embodiments]” to “make a meaningfully distinct contention.”); *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.’”) (internal citation omitted); *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,” that a purported “Foster[] DRMS” embodiment is evidence that content is “‘downloaded to [i.e., stored at a] personal computer’ for on-demand access.” Reply, 25. The Petition, however, never mentions any DRMS embodiment, much less storage on a PC. *See, e.g.*, Pet., 61-62 (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 abandoned Foster’s system in favor of Foster’s prior art confirms that the Petition did not establish a motivation to combine Foster-Hayhurst.

The Reply also argues that “Foster’s teachings include storage-based embodiments,” relying upon Foster’s description of an “MPEG-standard’s ‘program stream,’ which Foster says is intended for use ‘in fixed storage.’” Reply, 26. 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 encrypted data segments in a distributed manner.” Pet., 64. Hayhurst teaches such segments are distributed through a cable network, and Foster teaches, in that context, that **transport** streams, not program streams, are used. EX1006 [Foster], [0073] (“A transport stream is typically used in error-prone broadcast environments such as digital television.”); EX2046 [Bhattacharjee-2nd-Depo.], 30:16-31:10 (digital television includes cable and satellite). Program streams are thus irrelevant to Petitioner’s original combination.

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 this purported embodiment involves storing an entire content file on a personal computer for later on-demand viewing. *See* Reply, 25. Petitioner’s new argument fails for multiple reasons.

To begin, 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, 25-26. But this is not “Foster’s” invention; rather, the DRMS Petitioner points to is Foster’s prior art. *See id.*; EX1006 [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 (EX2046 [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.” EX1006 [Foster], [0051]; EX2034 [Bhattacharjee-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; not an embodiment of Foster's invention. Whether DRMS allegedly stores an entire content file on a personal computer has no bearing on whether Foster's system does. And to the extent that Petitioner proposes modifying Foster to use DRMS, Petitioner fails to explain why a POSITA would have been so motivated, given Foster's criticism of DRMS.

Nor does Petitioner explain how the *personal computer* used in DRMS would have a place in Foster-Hayhurst, which utilizes Hayhurst's decentralized distribution system for *set-top boxes*. Pet., 64. Petitioner provides no explanation for what its revised combination would be or 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 suggest that Foster teaches that the entire content file is stored on a personal computer in its system. Petitioner does not cite any embodiments of "fixed storage" in Foster, but merely states, without explanation or citation, that "Foster's text makes clear that Foster's teachings include storage-based embodiments." Such vague and conclusory statements cannot establish invalidity. *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.”).

Petitioner also argues that prior art 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, 26 (citing 11 paragraphs of reply-declaration and six new exhibits). But 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. See Reply, 26 (content can be stored on a “VOD server” or generic “storage media.”). And, even if it did, Petitioner does not explain why this would motivate a POSITA to combine Foster-Hayhurst.

IV. CONCLUSION

The claims should be confirmed.

Respectfully submitted,

/s/ 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* to be filed

Colette Woo, *pro hac vice* to be filed

LOWENSTEIN & WEATHERWAX LLP

Date: February 3, 2025

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Sur-Reply (the “Sur-Reply”) consists of 5,598 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,

/s/ Stephen J. Elliott

Stephen J. Elliott

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
Richard F. Giunta	RGiunta-PTAB@wolfgreenfield.com
Marc S. Johannes	MJohannes-PTAB@wolfgreenfield.com
Gregory S. Nieberg	GNieberg-PTAB@wolfgreenfield.com

Respectfully submitted,

/s/ Stephen J. Elliott

Stephen J. Elliott

Date: February 3, 2025