

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

Case No. IPR2025-00003
Patent No. 9,313,178

**PETITIONER'S OPPOSITION
TO PATENT OWNER'S MOTION TO AMEND**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE MTA VIOLATES 35 U.S.C. § 316(D) AND 37 C.F.R. § 42.121	2
	A. The Amendments Improperly Enlarge Claim Scope	2
	B. The Amendments Improperly Introduce New Matter.....	5
	1. [21.5] and [21.6] Introduce New Matter	6
	2. [21.2] Also Introduces New Matter	7
III.	THE SUBSTITUTE CLAIMS REMAIN UNPATENTABLE.....	8
	A. Ground 6A: Peterka-Traw	8
	1. Overview of Peterka.....	8
	2. Overview of Traw	9
	3. Reasons to combine Peterka and Traw	10
	4. Peterka-Traw Renders Obvious Substitute Claims 21-26 and 29-30.....	12
	a. Substitute Claim 21	13
	b. Substitute Claim 22.....	18
	c. Substitute Claim 23.....	19
	d. Substitute Claims 24-26 and 29	21
	e. Substitute Claim 30.....	21
	5. Peterka-Traw Render Obvious Substitute Claims 33-35, 37	22
	B. Additional Traw Combinations (Grounds 6B-6E).....	22
	C. Ground 7: Indefiniteness	22
	1. All claims: “the expiration time-based key rotation boundary previously provided for the content encryption key currently being used”	23
	2. All claims: “for the duration of the media playback”	23
	3. Claims 22-26 and 33-37: “second content key” in relation to “expiration times”.....	23
	D. Ground 8: Unpatentable Subject Matter.....	24

TABLE OF AUTHORITIES

CASES

<i>Alice Corp. v. CLS Bank Int’l</i> , 573 U.S. 208 (2014)	25
<i>Aqua Prods., Inc. v. Matal</i> , 872 F.3d 1290 (Fed. Cir. 2017) (<i>en banc</i>).....	2, 5
<i>Hawk Tech. Sys., LLC v. Castle Retail, LLC</i> , 60 F.4th 1349 (Fed. Cir. 2023)	25
<i>Int’l Bus. Machines Corp. v. Zillow Grp., Inc.</i> , 50 F.4th 1371 (Fed. Cir. 2022)	25
<i>K/S HIMPP v. Bragi GmbH</i> , IPR2023-01204, Paper 40 (PTAB Mar. 7, 2025).....	2
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	18, 19
<i>Lectrosonics, Inc. v. Zaxcom, Inc.</i> , IPR2018-01129, -01130, Paper 15 (PTAB Feb. 25, 2019) (precedential).....	2
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014)	23, 24
<i>Neuroderm Ltd. v. Abbvie Inc.</i> , PGR2022-00040, Paper 77 (PTAB Oct. 31, 2023)	5
<i>Pannu v. Storz Instruments, Inc.</i> , 258 F.3d 1366 (Fed. Cir. 2001)	4
<i>Red Diamond, Inc. v. Southern Visions, LLP</i> , IPR2019-01662, Paper 36 (PTAB Mar. 31, 2021).....	5
<i>Silencerco Weapons Rsch. Center v. Huxwrx Safety</i> , IPR2024-01214, Paper 22 (PTAB Aug. 18, 2025)	5
<i>Sisvel Int’l S.A. v. Sierra Wireless, Inc.</i> , 81 F.4th 1231 (Fed. Cir. 2023)	2, 3, 4

<i>Spectrum Sols. LLC v. DNA Genotek Inc.</i> , IPR2023-01424, Paper 45 (PTAB Feb. 19, 2025)	5
---	---

STATUTES

35 U.S.C. § 101	8, 25
35 U.S.C. § 102(a)(1).....	9
35 U.S.C. § 102(a)(2).....	9
35 U.S.C. § 103	8
35 U.S.C. § 112.....	8
35 U.S.C. § 316(d)	1, 2, 8
35 U.S.C. § 316(d)(3).....	2, 5, 7

REGULATIONS

37 C.F.R. § 1.175(b)	4
37 C.F.R. § 42.121	1, 2

OTHER AUTHORITIES

Manual of Patent Examining Procedure (MPEP) § 2106.04(a)-(d)	25
USPTO, Memorandum Re. Reminders on evaluating subject matter eligibility of claims under 35 U.S.C. 101 (Aug. 4, 2025)	25

LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 9,313,178 (“178 Patent”)
1002	Prosecution History of U.S. Patent No. 9,313,178 (“178 FH”)
1003	Declaration of Anthony J. Wechselberger (“Wechselberger”)
1004	Curriculum Vitae of Anthony J. Wechselberger (“Wechselberger-CV”)
1005	U.S. Patent Publication No. 2002/0172368 (“Peterka”)
1006	Certified Translation of Japanese Published Patent Application No. 2004-166153 (“Suzuki”)
1007	U.S. Patent Publication No. 2010/0235528 (“Bocharov”)
1008	U.S. Patent Publication No. 2008/0270308 (“Peterka308”)
1009	European Patent Publication No. 1,418,756 A2 (“Chen”)
1010	U.S. Patent Publication No. 2005/0138362 (“Kelly”)
1011	U.S. Patent No. 8,677,428 (“Lewis”)
1012	U.S. Patent No. 8,789,196 (“Pestoni”)
1013	International Publication No. WO 2010/107625 A2 (“Sood”)
1014	U.S. Patent No. 8,806,050 (“Chen050”)
1015	T. Stockhammer, “Dynamic adaptive streaming over HTTP: Standards and design principles,” in Proc. ACM MMSys’11, San Jose, CA, USA, Feb. 23–25, 2011, pp. 133–144 (“Stockhammer”)
1016	W. Van Lancker, D. Van Deursen, E. Mannens and R. Van de Walle, “HTTP adaptive streaming with Media Fragment URIs,” 2011 IEEE International Conference on Multimedia and Expo, Barcelona, Spain, 2011, pp. 1-6, doi: 10.1109/ICME.2011.6012149 (“Van Lancker”)
1017	3GPP TS 26.234 version 9.3.0 Release 9 (2010-06), Technical Specification, “Universal Mobile Telecommunications Systems (UMTS); LTE; Transparent end-to-end Packet Streaming Services (PSS); Protocols and codecs,” Reference RTS/TSGS-0426234v930 (June 2010) (“3GPP-AHS”)
1018	R. Pantos (Ed.), HTTP Live Streaming, draft-pantos-http-live-streaming-06 (Mar. 31, 2011) (“Pantos”)
1019	RFC793: Transmission Control Protocol (September 1981) (“RFC793”)
1020	RFC2616: Hypertext Transfer Protocol – HTTP/1.1 (June 1999) (“RFC2616”)

1021	The Secure Sockets Layer Protocol, V. 3.0, <i>available at</i> https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html and https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1 (“SSL-Standard”)
1022	U.S. Patent No. 8,756,673 (“Barrus”)
1023	Yuan et al., “Layered access control for MPEG-4 FGS video,” Proceedings 2003 International Conference on Image Processing (Cat. No. 03CH37429), Barcelona, Spain, doi: 10.1109/ICIP.2003.1247012 (“Yuan”)
1024	U.S. Patent App. Pub. No. 2005/0060316 (“Kamath”)
1025	RESERVED
1026	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 2 (Feb. 25, 2022)
1027	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 9 (July 8, 2022)
1028	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 11 (Sept. 1, 2022)
1029	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 13 (Nov. 28, 2022)
1030	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 14 (Nov. 28, 2022)
1031	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 17 (Dec. 30, 2022)
1032	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Order No. 25 (Mar. 13, 2024)
1033	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Complaint, Exhibit 24 (October 12, 2023)
1034	<i>Telefonaktiebolaget LM Ericsson et al. v. Lenovo</i> , 5:23-cv-00570, Order Granting Motion to Stay (E.D.N.C. Feb. 9, 2024)
1035	USPTO Binding Interim Guidance Addressing PTAB’s Approach to Discretionary Denials, June 21, 2022, <i>available at</i> https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621.pdf .
1036	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Final Initial Determination (Nov. 15, 2024)
1037	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Commission’s Determination Affirming ALJ’s Final Initial Determination (Jan. 16, 2025)

1038	Declaration of Turhan F. Sarwar in Support of Admission <i>Pro Hac Vice</i>
1039	Declaration of Elizabeth A. DiMarco in Support of Admission <i>Pro Hac Vice</i>
1040	Deposition Transcript of John Villasenor Ph.D. (August 21, 2025)
1041	Supplemental Declaration of Anthony J. Wechselberger
1042	U.S. Patent No. 7,392,381 (“Traw”)

I. INTRODUCTION

The Board should deny Paper No. 24 (“MTA”) because PO does not carry its burden and, in any event, the substitute claims remain unpatentable.

The ’178 Patent claims a key rotation system driven by “key rotation boundaries.” The boundaries dictate when a “first” (e.g., current) content encryption key (“CEK”) is discontinued and after which a “second” (e.g., next) CEK is applied. In the claimed system, a client device “issues requests to the license server ahead of” a key rotation boundary to retrieve a “second” CEK that will be “*applie[dl]*” “*after the key rotation boundary* is reached.”¹ EX1001, 2:22-30; *id.*, claims 1, 16.

The substitute claims fundamentally—and impermissibly—broaden the scope of the original claims by *eliminating* the requirement that a second CEK be applied *after the rotation boundary*. Instead, the substitute claims recite a different and broader requirement that the claimed second CEK is applied *before the rotation boundary*. The substitute claims also introduce new matter unsupported by the ’178 Patent’s specification. The substitute claims thus violate 35 U.S.C. § 316(d) and 37 C.F.R. § 42.121.

Separately, even if the substitute claims complied with Section 316(d) (they do not), the substitute claims remain unpatentable under Sections 103, 101, and 112.

¹ Emphasis added throughout unless otherwise specified.

II. THE MTA VIOLATES 35 U.S.C. § 316(d) AND 37 C.F.R. § 42.121

Petitioner bears the burden of demonstrating the unpatentability of any substitute claims. *Aqua Prods., Inc. v. Matal*, 872 F.3d 1290, 1296 (Fed. Cir. 2017) (*en banc*). However, PO bears the burden to demonstrate that the substitute claims comply with statutory and regulatory requirements. *See Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, -01130, Paper 15, at 4 (PTAB Feb. 25, 2019) (precedential) (before considering substitute claims “the Board first must determine whether the motion to amend meets the statutory and regulatory requirements set forth in 35 U.S.C. § 316(d) and 37 C.F.R. § 42.121”).

PO must demonstrate, among other requirements, that “the amendment does not seek to enlarge the scope of the claims of the patent and does not introduce new matter.” *K/S HIMPP v. Bragi GmbH*, IPR2023-01204, Paper No. 40, at 47-48 (PTAB Mar. 7, 2025). Here, PO cannot make such a demonstration.

A. The Amendments Improperly Enlarge Claim Scope

Claim amendments in an IPR “may not enlarge the scope of the claims of the patent.” 35 U.S.C. § 316(d)(3). A substitute claim “is broader in scope than the original claim[] if it contains within its scope any conceivable apparatus or process which would not have infringed the original patent.” *Sisvel Int’l S.A. v. Sierra Wireless, Inc.*, 81 F.4th 1231, 1237-38 (Fed. Cir. 2023) (reexamination and reissue standards apply to IPR proceedings). Whether an amendment enlarges claim scope

“is a matter of claim construction” and is “a question of law.” *Id.* at 1238.

Original claim 1 recites “issuing requests to a license server...to retrieve a second [CEK] to be *used after a [CEK] rotation boundary* is reached.” EX1001, claim 1. Claim 1 further requires “*applying* the second key for content decryption *after* the key rotation boundary is reached.” *Id.* A system that obtained a second CEK, applied that second CEK *before* the claimed content encryption key rotation boundary, and discarded that second CEK at or before the boundary (i.e., did not apply it after the boundary) would meet the requirements of this substitute claim yet *would not* meet the requirements of the original claim. EX1041, ¶282.

Substitute limitations [21.5]-[21.6] *change* the recited CEK “rotation boundary” recited in claim 1 and *eliminate* the critical claim limitation that the second CEK be applied *after reaching the rotation boundary*:

[21.5] issuing requests to a license server in response to detecting said notification-based content encryption key rotation boundary ahead of a the expiration time-based key rotation boundary previously provided for the content encryption key currently being used to retrieve a second content encryption key to be used ~~after a~~ before said expiration time-based content encryption key rotation boundary for the content encryption key currently being used is reached; and

[21.6] applying the second key for content decryption ~~after the~~ before said expiration time-based key rotation boundary for the content encryption key currently being used is reached.

MTA, 16 (yellow highlighting added). Substitute claim 21 replaces that limitation with a broader limitation requiring the application of the second CEK *before* “said expiration time-based key rotation boundary.” *Id.* (underlining original).

There is no question that applying a second CEK *before* a key rotation

boundary *materially differs from* applying a second CEK *after* a key rotation boundary. EX1041, ¶282. PO's own expert admitted at deposition that switching the "*after*" to "*before*" in the original claims is "literally not what the [original] claim says." EX1040, 42:25-43:23. By deleting original claim 1's requirement of applying a second CEK *after* the CEK rotation boundary and replacing it with a *different* requirement, claim 21 is impermissibly "broader in [at least] that respect." *Pannu v. Storz Instruments, Inc.*, 258 F.3d 1366, 1371 (Fed. Cir. 2001) ("[A] claim that does not include a limitation present in the original patent claims is broader in that respect.").

Critically, this broadening is dispositive even if the substitute claim "may be narrower in other respects." *Sisvel Int'l*, 81 F.4th at 1241 ("[I]f a substitute claim is broader *in any respect* it is...broader than the original claim even though it may be narrower in other respects.") (emphasis original, internal quotation omitted); see 37 C.F.R. § 1.175(b) (similar).

The Board has routinely rejected similar substitute claims as impermissibly broadening. See *Sisvel Int'l*, 81 F.4th at 1239-40 (substitute claim was broader than original claim where substitute claim replaced requirement that claimed value be set "*based at least in part on information in* at least one frequency parameter" with a requirement that claimed value be set "*using the* frequency parameter"); *Silencerco Weapons Rsch. Center v. Huxwrx Safety*, IPR2024-01214, Paper 22, at 5 (PTAB

Aug. 18, 2025) (preliminarily rejecting as broadening a substitute claim that “delete[d] ‘high energy device’ and replace[d] it with ‘weapon’”); *Spectrum Sols. LLC v. DNA Genotek Inc.*, IPR2023-01424, Paper No. 45, at 9-14 (PTAB Feb. 19, 2025) (denying motion to amend on broadening grounds).

PO makes no meaningful effort to meet its burden. The MTA’s unsupported assertion that the substitute claims retain all original features (MTA, 2) is plainly incorrect, yet the MTA fails to even acknowledge—let alone justify—this change in claim scope. *See* MTA, 2-3.

PO’s deletion of the term “after” relative to the application of the second CEK improperly broadens the scope of the original claims. The error permeates all proposed substitute claims. Thus, the Board should deny the MTA in entirety.

B. The Amendments Improperly Introduce New Matter

PO also bears the burden in an IPR to establish that claim amendments do not introduce new matter. *Aqua Prods.*, 872 F.3d at 1305-06 (“[P]atent owner must satisfy the Board that the statutory criteria in...§ 316(d)(3) are met.”) (lead plurality opinion); *Neuroderm Ltd. v. Abbvie Inc.*, PGR2022-00040, Paper 77, at 14-15 (PTAB Oct. 31, 2023) (rejecting substitute claim where PO failed to show proposed amendment did not introduce new matter); *Red Diamond, Inc. v. Southern Visions, LLP*, IPR2019-01662, Paper 36, at 21-22 (PTAB Mar. 31, 2021) (same). PO acknowledges its burden (MTA, 9-10) but fails to meet it.

1. [21.5] and [21.6] Introduce New Matter

[21.6] recites “applying the second key for content decryption ~~after the~~ before said expiration time-based key rotation boundary for the [CEK] currently being used is reached.” MTA, 16. The MTA (at 10) alleges that the following paragraphs of the ’178 Application (EX2007) support [21.6]: ¶¶5, 36, 39; Fig. 3; cl. 1, 16. None do.

Every original claim required that a second key be applied for decryption *after* the rotation boundary, and no original claim required that a second key be applied for decryption *before* any rotation boundary. Likewise, the MTA’s cited paragraphs do not support the amendments in [21.6]. Paragraph 5 mimics original claim 1:

the client device detects content encryption key rotation boundaries... issues requests to the license server ahead of a key rotation boundary to *retrieve a second content encryption key*...and applies the second key for content decryption *after the key rotation boundary is reached*.

EX2007, ¶5.

Paragraph 36 describes checking the expiration of a “current content key to see if a new key should be applied.” Paragraph 39 similarly describes checking CEK expiration and the process for requesting a new CEK. While these two paragraphs generally describe (and Figure 3 illustrates) “two cases—normal period-based expiration, and an explicit key change notification,” (*id.* ¶39) there is *no description* of applying a second key for decryption *before* any rotation boundary.

Nor would such a requirement make sense. In the “normal period-based expiration” case, the second key is applied for decryption *after* a rotation boundary.

And in the “explicit key change notification” case, replacement keys are requested independent of and, agnostic to, key rotation boundaries. Beyond conclusory assertions in a table, PO makes no attempt to demonstrate that a POSA would have understood the specification in a way that supports the new limitations.

[21.5] likewise fails because the MTA’s purported support never describes issuing requests for a second key to be used before any key rotation boundary. PO offers no explanation for how such disclosures support the new limitation. *See* EX2007, ¶¶3, 5, 8-9, 21, 26, 32, 35-36, 39; Fig. 3; cls. 1, 12-16, 20.

[21.5] and [21.6] thus introduce new matter in violation of § 316(d)(3).

2. [21.2] Also Introduces New Matter

[21.2] recites “parsing content information from the playback request response, the content information including...[CEK] identifiers that uniquely identify each [CEK] from every other [CEK] for the duration of the media playback.” MTA, 15. As purported support, the MTA cites ¶¶3, 5, 8, 10, 20, 36; cls. 1, 16. Here again, PO fails to carry its burden.

Original claims 1 and 16 did not include the requirement added to [21.2]. EX2007’s sole description of “[CEK] identifiers” appears in Paragraph 8: “Each [CEK] in the history is assigned a unique identifier which is referred to herein as the [CEK] identifier.” The parties dispute the meaning of “unique identifier.” *Compare* Pet., 25-26, *with* POR, 37-39. Regardless of that dispute, the ’178 Application

indisputably *does not describe* the *duration* for which the uniqueness of any “identifier” must be maintained. EX1041, ¶¶311-313. For example, POSAs understood the “history” described in the specification could—for programs with “long or indefinite durations” (EX2007, ¶2)—be shorter than the entire duration of media playback. EX1041, ¶313. [21.2] thus adds new matter, and the MTA should be denied.

III. THE SUBSTITUTE CLAIMS REMAIN UNPATENTABLE

Apart from failing comply with 35 U.S.C. § 316(d), the substitute claims should be rejected as unpatentable for: (1) obviousness under Section 103; (2) indefiniteness under Section 112; (3) claiming unpatentable subject matter under Section 101.

A. Ground 6A: Peterka-Traw

Substitute claims 21-26, 29-30, 33-35, and 37 are obvious over Peterka in view of Traw (“Peterka-Traw”). The proposed claim amendments recite requesting, receiving, and applying a second CEK *before* reaching the current key’s rotation boundary. This basic concept was described long before the ’178 Patent’s priority date, including in U.S. Patent No. 7,392,381 (EX1042, “Traw”). The remaining amendments recite non-functional descriptions, intended purposes, or are otherwise disclosed by Peterka.

1. Overview of Peterka

Peterka (EX1005) relates to securely distributing multimedia content over a

network. Peterka, Abstract, FIG. 1, [0038], [0006]-[0012]. Peterka’s “client” devices download streaming media from a content distribution system. *Id.*, [0038]. Media content is divided into segments that are each encrypted with a different key. *Id.*, [0080]-[0082], [0091]-[0101], [0122]-[0125], FIGs. 7A-7B. These encrypted media segments are streamed to clients. Peterka, [0043], [0119].

Peterka’s client obtains and applies the key required to decrypt each media segment—e.g., a content key (“CK”). *Id.*, [0011], [0091]-[0093], [0127], FIG. 7A; Wechselberger, ¶50. Peterka describes obtaining such keys through a pull model in which a client tracks its keys and their expiration times and actively requests new/replacement keys as needed. Peterka, [0105]-[0106]; Wechselberger, ¶¶51-52.

2. Overview of Traw

Traw was filed April 13, 2004, issued on June 24, 2008, and is 35 U.S.C. § 102(a)(1)-(2) prior art. Traw is directed to a content protection system that both rotates keys “on a periodic basis” *and* “generate[s] revocation data corresponding to revoked keys in response to... a security compromise.” Traw, Abstract; *see id.*, 1:65-2:6 (key “revocation is also used to prevent access to content if the devices’ keys have been compromised”), 4:37-39. Traw’s system thus “protect[s] content (such as audiovisual entertainment content) against unauthorized access, copying or distribution.” *Id.*, 2:15-19. Traw’s system is “especially” suited for devices that “include software for assisting in implementing content protection” where “software

may be updated via a communication mechanism” like the internet. *Id.*, 2:19-51.

Traw describes two types of key revocation in which current content keys are replaced: (1) periodic/planned key revocation (Traw, 5:33-35, 6:10-12); and (2) non-periodic/unplanned key revocation based on compromised keys, security attacks, or emergency situations (*id.*, 3:65-66, 4:37-39, 5:5-7, 5:37-39, FIG. 2). Messages are transmitted “to users and/or devices announcing” the key revocation. *Id.*, 5:63-65.

3. Reasons to combine Peterka and Traw

POSAs would have had numerous reasons to modify Peterka to incorporate Traw’s key revocation techniques and would have reasonably expected success in doing so. EX1041, ¶262; *see also id.*, ¶¶243-256.

First, Peterka and Traw are in the same field of art. EX1041, ¶¶263-264. Both describe systems that distribute secure content encrypted with content keys and changing/rotating those keys. *Compare* Traw, Abstract, 1:65-2:2, 2:56-60, 3:13-19, 4:11-14, *with* Peterka, [0116]-[0121], FIG. 14. Both teach providing content keys to clients for decryption. *Compare* Traw, 3:63-66, 4:11-14, 5:5-19, FIGs. 1-3 *with* Peterka, [0080], [0105]-[0106], [0130], FIGs. 7B, 8. And both teach an identification mechanism for managing keys (e.g., “sequence number or time stamp” in Peterka and “key IDs” in Traw). *Compare* Traw, 3:32-46, *with* Peterka, [0082], [0110].

Second, Peterka and Traw share common objectives to prevent unauthorized access to content. *Compare* Peterka, [0135]-[0146] (describing “rules and conditions

for providing content in a multicasting environment” to authorized clients), *with* Traw, 2:15-19 (describing protecting content from “unauthorized access”). Peterka recognizes the risk of security attacks and provides security mechanisms to protect against them—e.g., periodically rotation keys “at regular intervals,” “a time stamp” in key-distribution ECMs “to protect against replay attacks.” Peterka, [0105], [0110], [0121]; EX1041, ¶¶265-266. Traw likewise recognizes the benefits of periodic key renewals. *E.g.*, Traw, 3:63-66 (“[R]evocation of keys may be performed proactively on a periodic basis, rather than only reactively in response to an attack.”).

Third, POSAs understood well that notwithstanding Peterka’s described security mechanisms including key rotation, the security of systems like Peterka’s could be improved to address breaches. *See* EX1040 (Villasenor Dep.), 135:20-136:5, 139:7-140:24; *see also id.*, 136:6-25. For example, Traw recognizes the benefits of “non-scheduled revocation” in systems like Peterka’s, including for keys that “have been compromised” (*id.*, 6:39-49) and to protect against “a more general set of threats” or attacks (*id.*, 6:49-57). Peterka leaves to POSAs’ discretion how to rectify a security attack. *See* Peterka, [0110]; EX1041, ¶¶266-267. POSAs understood from Traw that compromised keys should be revoked, including in systems like Peterka with key rotation. Traw, 6:39-56; EX1041, ¶267. POSAs also understood that Traw’s security-driven key revocation teachings complement and support Peterka’s goal of limiting media access to authorized users—a goal Traw

itself shares. EX1041, ¶267.

POSAs thus would have been motivated to improve Peterka’s system (*see* EX1040, 135:20-136:5, 139:7-140:24; *see also id.*, 136:6-25) in view of Traw by: (1) providing a notification to clients that a certain key is compromised and requires early expiration (Traw, 5:63-65, 4:62-65) using Peterka’s content packet “signaling methods” for key changes (Pet., 11; Peterka, [0116]-[0120]); (2) having the client obtain a replacement key using Peterka’s “pull” method (Pet., 11-12; Peterka, [0105]-[0106]) when notified that the current key has been revoked before the originally-scheduled expiration of the compromised key (Traw, 6:18-21); and (3) having the client apply the replacement key for decryption when the replacement key is received, before the originally-scheduled expiration of the compromised key in order to minimize service interruptions (Peterka, [0105]). EX1041, ¶268.

This modified system—“Peterka-Traw”—would have maintained Peterka’s overall system while beneficially improving security by including a mechanism to handle successful security attacks—namely, revoking and requiring replacement of a compromised key before it is set to expire (as taught by Traw). EX1041, ¶268.

POSAs would have reasonably expected success with Peterka-Traw, because Traw teaches a straightforward way to address security breaches easily adaptable to Peterka. EX1041, ¶269; Peterka, [0105]-[0106], [0116]-[0121], [0135]-[0138].

4. Peterka-Traw Renders Obvious Substitute Claims 21-26 and 29-30

a. Substitute Claim 21

Substitute claim 21 amends original independent claim 1. *See* MTA, 15-16. Unchanged claim limitations are obvious for the reasons set forth in Ground 1. Pet., 19-37; EX1041, ¶¶270-289. Amended limitations are obvious over Peterka-Traw.

[21.P] adds a non-limiting statement of use: “for over-the-top [(‘OTT’)] media delivery.” Peterka-Traw satisfies [21.P] for the same reasons Peterka satisfies [1Pre]. Pet., 19. To the extent “for [OTT] media delivery” is limiting, Peterka-Traw satisfies it based on Peterka’s teaching to rotate keys in OTT streaming. *See* Pet., 3, 57; Peterka, [0015], [0038], FIG. 1; Wechselberger, ¶178; EX1041, ¶270.

[21.1] and [21.3] are unchanged. Peterka-Traw satisfies [21.1] and [21.3] for the same reasons Peterka satisfies [1A] and [1C], respectively. Pet., 19-22 ([1A]), 28-31 ([1C]); EX1041, ¶¶272, 278.

[21.2] adds a requirement that the CEK identifiers “uniquely identify each [CEK] from every other [CEK] for the duration of the media playback.” While there is no intrinsic support for this interpretation (let alone written description support as discussed *supra* § II.B.2), Peterka-Traw satisfies this requirement.

Peterka-Traw includes Peterka’s sequence number or timestamp delivered to a client along with a CEK in an ECM/EMM, each of which POSAs understood constitutes a unique CEK identifier that can be used to identify the key in the ECM/EMM. Pet., 25-26; Peterka, [0121]; Wechselberger, ¶¶91-92; EX1041, ¶274.

This understanding of CEK identifier is consistent with the '178 Patent, which likewise describes key identifiers “selected based on” other data such as “a segment number of the prepared content.” EX1001, 3:34-35, 4:8-10, 6:1-3, 6:17-19.²

Because Peterka’s “sequence number” or “timestamp” is specifically included “*to protect against replay attacks*” during media playback (Peterka, [0121]), POSAs also would have understood that each sequence number/timestamp “uniquely identif[ies] each” ECM/EMM (and “[CEK]” within) “from every other” ECM/EMM and corresponding “[CEK] *for the duration of the media playback.*” EX1041, ¶274.

Moreover, ensuring uniqueness of key identifiers “for the duration of the media playback” would have been obvious. EX1041, ¶275. POSAs would have been motivated (and reasonably expect success) to ensure a client could uniquely identify keys even in scenarios where the client ultimately acquired all the keys needed for the entire duration of media playback. *E.g.*, EX2011 (Wechselberger Tr.), 39:7-40:13 (the “need to identify” and “know which key to use when” is “fundamental” to “anybody who has worked with crypto-based content information distribution

² While PO tries to dismiss Peterka’s sequence numbers/timestamps as merely “message identifiers” because they are not “assigned” to a key (POR, 39), no “assignment” requirement is recited in the original or substitute claims. PO identifies no basis to depart from the plain meaning of CEK identifier.

systems”); Pet., 25-26; Wechselberger, ¶¶94-96 (citing Suzuki, [0013], [0016], [0030]-[0031], [0043]-[0048], [0080]-[0084], FIG. 5; Pestoni, 12:16-35); EX1041, ¶276.

Peterka *itself* illustrates such a scenario in FIG. 7B by showing content key identifiers—CK₀, CK₁, CK₂—that are unique for the entire program’s duration. Peterka, FIG. 7B; *id.*, FIG. 7A, [0092] (FIG. 7A “illustrate[s] an example where only two keys are required to decrypt the remainder of the program”); EX1041, ¶276. POSAs would have reasonably expected success using identifiers sufficiently unique to distinguish between CKs over the duration of media playback given Peterka’s teachings (Peterka, [0092], FIGs. 7A-7B) and because it was common to use key IDs sufficiently unique to allow clients to keep track of keys required to playback a piece of content. EX1041, ¶77; Pestoni, 12:4-35, FIG. 4.

[21.4] adds the requirement of detecting “notification-based [CEK] rotation boundaries” wherein “a notification requires expiration of a [CEK] currently being used earlier than the content key expiration time previously provided for that key.” By focusing on the compromised key scenario and an explicit key change notification that requires key rotation outside the period-based boundary (MTA, 10), [21.4] attempts to change the meaning ascribed to the “detecting” limitation in the same way that PO asserts the original “detecting” limitation should be construed. POR, 43-49.

Regardless, Peterka-Traw satisfies this limitation. EX1041, ¶279. Traw teaches revoking a key that has been compromised due to a security breach *before* that key would ordinarily be rotated (Traw, 3:17-19, 5:35-39, 6:12-21, 6:39-57) and notifying client devices of such revocations (*id.*, 4:62-65, 5:63-65). EX1041, ¶280. In Peterka-Traw, notifications of these unscheduled key revocations are transmitted to (and detected by) the client using Peterka’s key change signaling methods. EX1041, ¶281; Peterka, [0116]-[0120]. Peterka-Traw’s client thus detects notification-based content encryption key rotation boundaries where the notification requires early expiration of the current content encryption key. EX1041, ¶281.

[21.5] adds the requirement that the client issues requests to the license server “in response to detecting said notification-based [CEK] rotation boundary ahead of a the expiration time-based key rotation boundary previously provided for the [CEK] currently being used to retrieve a second [CEK] to be used ~~after~~ before said expiration time-based [CEK] rotation boundary for the [CEK] currently being used is reached.” PO’s amendments in [21.5] are again aimed at capturing the “compromised key” scenario discussed above for [21.4], and, as discussed *supra* § II.B.1, improperly broaden the claim by changing *when* the second CEK is applied. Moreover, as discussed *infra* § III.B.1, there is no antecedent basis for the purported “expiration time-based key rotation boundary.”

To the extent not indefinite, Peterka-Traw satisfies this clause. EX1041, ¶282.

In Peterka-Traw, the client keeps track of its keys and issues requests for new keys in a manner that avoids “service interruptions.” Peterka, [0105]. POSAs would have been motivated to implement Peterka-Traw such that when the client detects an unscheduled key revocation taught by Traw (Traw, 3:17-19, 5:35-39, 6:12-21, 6:39-57; *see also id.*, 4:63-65, 5:63-65) using Peterka’s key change signaling methods (Peterka, [0116]-[0120]), Peterka-Traw’s client requests a new key immediately, before the current (compromised key) is set to expire. This would minimize the impact of service interruption, as Peterka teaches (Peterka, [0105]). EX1041, ¶¶283-286. Such a request would satisfy [21.5].

[21.6] changes the requirement from original claim 1 to apply the second key for content decryption from “after the key rotation boundary” to “~~after the~~ before said expiration time-based key rotation boundary for the [CEK] currently being used is reached.” As described *infra* § III.B.1, there is no antecedent basis for the purported “expiration time-based key rotation boundary.”

To the extent not indefinite, Peterka-Traw satisfies this. EX1041, ¶¶287-288. To minimize “service interruptions” (Peterka, [0105]), POSAs would have been motivated to implement Peterka-Traw such that when the client receives the second (replacement) key due to Traw’s unscheduled key revocation (Traw, 3:17-19, 4:63-65, 5:35-39, 5:63-65, 6:12-21, 6:39-57), the client promptly applies the second key for decryption, before the current key is set to expire, allowing the client to resume

consuming content. EX1041, ¶289; Peterka, [0106], [0116]; Wechselberger, ¶124.

Thus, Peterka-Traw renders substitute claim 21 obvious. EX1041, ¶¶270-289.

b. Substitute Claim 22

Substitute claim 22 mirrors original dependent claim 2. *See* MTA, 16. Unchanged claim limitations are obvious for the reasons set forth in Ground 1. Pet., 37; EX1041, ¶290. Claim 22 adds the requirement that the CEK expiration time for the second CEK is “equal to the time remaining for the expiration previously set for the prior [CEK].” Peterka-Traw satisfies this limitation. EX1041, ¶291.

POSAs would have understood that there were three options for setting the expiration time of a replacement key: (1) ***before*** the expiration of the original key; (2) ***at the same time*** as the original key expiration; or (3) ***after*** the expiration of the original key. EX1041, ¶292. All three options would have been obvious to try. EX1041, ¶¶292-293; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007).

POSAs had multiple reasons to try setting the second CEK’s expiration time to be equal to the time remaining for the expiration set for the prior CEK. ***First***, the expiration time of the prior (compromised) CEK was already known to both the client and server, and setting the CEK expiration time for the second CEK as equal to the time remaining for the prior CEK would minimize the need to adjust any existing time variables associated with the upcoming key rotation. EX1041, ¶294.

Second, adjusting the second CEK’s expiration time such that it was not the

same time as the prior CEK would have required changing already-staged key rotation boundaries that are tied to future media segments, including interstitial segments like ads, previews, etc. that were common in multicast content distribution. Peterka, [0122], FIG. 7B; EX1041, ¶295 (citing Peterka308, [0024], [0029], [0032]; Chen [0034]-[0044], FIGs. 2A-2C). Using the expiration time of the original key would avoid the need to adjust these already-staged key rotation boundaries.

Further, given Traw's disclosure that its revocation can target a single key (Traw, 3:35, 4:45), POSAs would have reasonably expected success revoking a single key and replacing it, leaving all other variables alone. EX1041, ¶296.

c. Substitute Claim 23

Substitute claim 23 mirrors original dependent claim 3 but adds the requirement that the second CEK's expiration time is "equal to the time remaining for the expiration previously set for the prior [CEK] *plus* the fixed expiration period duration originally assigned for the prior [CEK]." See MTA, 16. Unchanged claim limitations are obvious for the reasons set forth in Ground 1. Pet., 38-41.

Claim 23's amendment falls within option #3 described above for substitute claim 22: expiration for the second (replacement) CEK *after* the expiration of the prior (compromised) key. EX1041, ¶¶297-299. As noted above, setting the second CEK's expiration time for *after* the prior (compromised) CEK's expiration was one of three obvious-to-try options. EX1041, ¶299; KSR, 550 U.S. at 421. POSAs would

have understood that setting the second CEK to both be applied *before* the prior (compromised) key expires³ and then expire *after* the prior CEK would have expired⁴ would mean that the CEK originally staged to be applied to the next media segment—possibly already distributed to some clients—was no longer usable for the upcoming segment. EX1041, ¶300.

To address this, POSAs would have been motivated to set the second CEK’s expiration time to be equal to the time remaining for the pre-existing expiration set for the prior CEK plus the fixed expiration period duration originally assigned for the prior CEK. This would provide Peterka-Traw’s servers an additional key rotation period to better handle potential latency issues that would predictably arise from numerous clients attempting to replace the compromised key *and* the now-defunct key that was originally staged. EX1041, ¶300; Peterka, [0080] (noting the issue of “a large load on the caching server on the segment boundaries”). This implementation also would avoid disrupting the encryption/decryption of future media segments by desirably allowing POSAs to avoid adjusting already-staged key rotation boundaries. Peterka, [0122], FIG. 7B; EX1041, ¶300 (citing Peterka308, [0024], [0029], [0032]; Chen [0034]-[0044], FIGs. 2A-2C).

³ As discussed *supra* § III.A.4.a, this was obvious and would have satisfied [21.6].

⁴ As discussed *supra*, this was obvious to try.

POSAs also would have reasonably expected success with such an implementation because it involves using less than two key rotation periods to give servers the chance to resume regular key distribution processes. EX1041, ¶301.

d. Substitute Claims 24-26 and 29

Claims 24-26, and 29 are unchanged. Peterka-Traw satisfies claims 24-26, and 29 for the same reasons that Peterka satisfies claims 4-6, and 10, respectively. Pet., 41-47 (discussing claims 4-6, and 10 as obvious over Peterka); EX1041, ¶302.

e. Substitute Claim 30

Substitute claim 30 amends dependent claim 12 and mirrors its structure but adds the following limitations: “retrieved content is divided into content segments, and said key is applied to decrypt the same content segment for which the previous [CEK] was used” and “early expiration of the [CEK] currently being used is for security reasons.” See MTA, 17-18. Claim 30’s unchanged limitations are obvious for the same reasons set forth in Ground 1. Pet., 48. Peterka-Traw renders obvious the amended limitations. EX1041, ¶¶303-306.

Peterka discloses content divided into segments encrypted (and decrypted) with a different key. Pet., 10, 36-37; Peterka, [0080]-[0082], [0091]-[0101], [0106], [0116], [0121]-[0125], FIGs. 7A-7B. Peterka’s modified system in Peterka-Traw includes a mechanism for responding to security attacks: revoking and requiring replacement of a compromised key before its set expiration. The second CEK is used to decrypt content originally slated to be decrypted by the prior (compromised) CEK,

and the early expiration of the prior (compromised) CEK is for security reasons.

Traw, 1:65-2:2, 2:15-19, 3:65-66, 4:37-39, 5:5-39, FIG. 2; EX1041, ¶¶305-306.

5. Peterka-Traw Render Obvious Substitute Claims 33-35, 37

Substitute claim 33 amends original claim 16 the same way substitute claim 21 amends claim 1. MTA, 18-19. Peterka-Traw's computerized device satisfies substitute claims 33-35 and 37 for the same reasons described above for proposed substitute claims 21-23 and 30. EX1041, ¶307.

B. Additional Traw Combinations (Grounds 6B-6E)

POSAs would also have combined Traw with the original grounds set forth in the Petition (Grounds 2-5), for the same reasons discussed *supra* § III.A.3. EX1041, ¶308. The resulting combinations (Peterka-Suzuki-Traw, Peterka-Bocharov-Traw, Peterka-Suzuki-Bocharov-Traw, Peterka-Bocharov-Peterka308-Chen-Traw) meet substitute claims 21-26, 29-30, 33-35, and 37 for the same reasons discussed *supra* § III.4, ***and also*** meet substitute claims 27-28, 32, and 36 for the reasons discussed in Grounds 2-5, as summarized below:

Ground and Reference(s)		Substitute Claims
6B	Peterka, Suzuki, Traw	21-26, 29-30, 33-35, 37
6C	Peterka, Bocharov, Traw	21-26, 29-30, <u>32</u> -35, 37
6D	Peterka, Suzuki, Bocharov, Traw	21-26, 29-30, <u>32</u> -35, 37
6E	Peterka, Bocharov, Peterka308, Chen, Traw	<u>27-28</u> , <u>36</u>

C. Ground 7: Indefiniteness

The substitute claims are indefinite because they (1) include terms that lack

antecedent basis and/or (2) introduce impermissible ambiguity. They thus “fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014).

1. All claims: “the expiration time-based key rotation boundary previously provided for the content encryption key currently being used”

Substitute limitations [21.5] and [33.7] lack proper antecedent basis for the phrase “the expiration time-based key rotation boundary previously provided” because the claims never introduce any such concept before [21.5] and [33.7]. Substitute limitations [21.4]/[33.5] instead recite detecting “**notification-based [CEK] rotation boundaries**.” Because substitute claims 21/33 provide no antecedent basis for the purported “expiration time-based key rotation boundary” prior to [21.5]/[33.7], it is unclear to POSAs what “the expiration time-based key rotation boundary” is, when it is provided, and what it does. EX1041, ¶309. All substitute claims include this requirement and are thus indefinite.

2. All claims: “for the duration of the media playback”

Substitute claims 21/33 recite “from every other [CEK] for the duration of the media playback.” This phrase lacks antecedent basis, rendering all claims indefinite, especially given that the claims cover playback of indefinite durations. EX1041, ¶¶310-313.

3. Claims 22-26 and 33-37: “second content key” in relation to “expiration times”

Substitute claims 22/33 recite receipt of a playback request response including content information that includes both “[CEKs]” and “[CEK] expiration times.” Those requirements appear in the original claims. PO’s amendments add a separate requirement to claims 22/33, wherein a CEK that was received in the playback request response is replaced—after a notification to do so—by a “second” CEK. The “second” CEK is obtained through a separate request and response. *See* MTA, 16, 19.

Dependent claims 2-6, 9, and 17-18 recite additional requirements relating to the CEK expiration times in the playback request response’s content information. Substitute dependent claims 22-26 and 33-37 amend the original claims to add limitations relating to the “second” CEK obtained through the separate process.

PO thus conflates the two separate claimed requests/responses creating an unresolved ambiguity. For the same reasons, the phrase “**the content key expiration time for said second [CEK]**” lacks antecedent basis. EX1041, ¶¶314-317. Claims 22-26 and 33-37 thus conflate claim requirements and cannot be reasonably understood, rendering them indefinite. *Nautilus*, 572 U.S. at 901.

D. Ground 8: Unpatentable Subject Matter

Under the latest USPTO Guidance, patentable subject matter requires consideration of two questions: (1) whether the claim recites any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain

methods of organizing human activity such as a fundamental economic practice, or mental processes) (“Step 2A, Prong One”); and (2) whether the claim recites additional elements that integrate the judicial exception into a practical application (“Step 2A, Prong Two”). USPTO Aug. 4, 2025 Memo. Regarding Section 101; MPEP §2106.04(a)-(d). The substitute claims here fail both prongs. EX1041, ¶318.

At the outset, there is no substantive difference between the method claims (22-29) and computerized device claims (33-37), and all substitute claims should be considered together for patent eligibility purposes.

The substitute claims fail Step 2A, Prong One because they are directed to the abstract idea of using CEKs to encrypt and decrypt information (media content segments) using a general-purpose computer as “merely... a tool.” *Int’l Bus. Machines Corp. v. Zillow Grp., Inc.*, 50 F.4th 1371, 1377 (Fed. Cir. 2022). The claims recite purely functional claim elements not tied to any improvement in computer architecture or functionality. Such “result-based functional language” as to “abstract data manipulation” fails. *Hawk Tech. Sys., LLC v. Castle Retail, LLC*, 60 F.4th 1349, 1357 (Fed. Cir. 2023).

The substitute claims also fail Step 2A, Prong Two as they do not recite any additional elements that integrate the judicial exception into a practical application. Instead, the substitute claims merely recite the use of generic, conventional computer technology. *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 217-218 (2014).

Respectfully submitted,
Google LLC

Date: September 5, 2025

/s/ Elizabeth A. DiMarco

Elizabeth A. DiMarco, admitted *pro hac vice*
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6 (e)(4)

I certify that on September 5, 2025, a copy of the foregoing document, including any exhibits filed therewith, is being served via electronic mail, as previously consented to by Patent Owner, upon the following:

Peter C. Knops
Kayvan B. Noroozi

peter@noroozipc.com
kayvan@noroozipc.com

Date: September 5, 2025

/Dara Del Rosario/
Dara Del Rosario
Paralegal
WOLF, GREENFIELD & SACKS, P.C.