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

_____

**SECOND SUPPLEMENTAL DECLARATION OF ANTHONY J. WECHSELBERGER IN SUPPORT OF PETITIONER'S OPPOSITION TO PATENT OWNER'S REVISED MOTION TO AMEND**

Google Exhibit 1047
Google v Ericsson
IPR2025-00003

# TABLE OF CONTENTS


I. SUMMARY OF OPINIONS ..... 2
II. PERSONAL AND PROFESSIONAL BACKGROUND ..... 3
III. MATERIALS REVIEWED AND CONSIDERED ..... 3
IV. MY UNDERSTANDING OF PATENT LAW ..... 6
V. BACKGROUND ..... 6
VI. PERSON OF ORDINARY SKILL IN THE ART ..... 7
VII. CLAIM INTERPRETATION ..... 7
VIII. PRIOR-ART REFERENCES ..... 8
IX. THE REVISED SUBSTITUTE CLAIMS ARE UNPATENTABLE ..... 8
A. Ground 6A: Peterka in view of Traw Renders Revised Substitute Claims 21-26, 29-30, 33-35, and 37 Obvious ..... 9
1. Peterka-Traw ..... 9
2. Claim-by-Claim Analysis ..... 9
a. Revised Substitute Claim 21 ..... 9
i. [21.P] ..... 10
ii. [21.1] ..... 11
iii. [21.2] ..... 11
iv. [21.3] ..... 19
v. [21.3A] ..... 19
vi. [21.4] ..... 21
vii. [21.5] ..... 23
viii. [21.6] ..... 29
b. Revised Substitute Claim 22 ..... 30
c. Revised Substitute Claim 23 ..... 33
d. Revised Substitute Claims 24-26 and 29 ..... 35
e. Revised Substitute Claim 30 ..... 35
f. Revised Substitute Claims 33-35 and 37 ..... 37
B. Additional Traw Combinations (Grounds 6B-6E) ..... 38
X. CONCLUSION ..... 42

I, Anthony J. Wechselberger, declare:

321. I executed a declaration on September 30, 2024 (EX-1003, ¶¶ 1-223, "Original Declaration" or "Orig. Decl.") in support of the Petition for *Inter Partes* Review of claims 1-8, 10, 12, 14, and 16-20 (the "Challenged Claims") of U.S. Patent No. 9,313,178 ("the '178 Patent") (Paper 3) filed by Petitioner Google LLC ("Google" or the "Petitioner") in this proceeding. I was cross-examined by deposition in connection with my Original Declaration on May 29, 2025. *See* EX-2011.

322. Petitioner asked that I consider certain new arguments raised by Patent Owner, Ericsson AB ("Patent Owner") in an Initial Motion to Amend (Paper 24, "IMTA") after I provided my Original Declaration. I executed an initial supplemental declaration on September 5, 2025 (EX-1041, ¶¶ 224-320, "Initial Supplemental Declaration" or "Initial Supp. Decl.") to address arguments raised in Patent Owner's IMTA and to provide opinions relating to the unpatentability of Patent Owner's proposed initial substitute claims 21-37.

323. Petitioner has asked that I consider certain new arguments raised by Patent Owner in a Revised Motion to Amend (Paper 32, "RMTA") after I provided my Original Declaration and Initial Supplemental Declaration. I submit this Second Supplemental Declaration to address arguments raised in Patent Owner's RMTA

and to provide opinions relating to the unpatentability of Patent Owner's proposed revised substitute claims 21-37 ("Revised Substitute Claims").

## I. SUMMARY OF OPINIONS

324. My opinions set forth in my Original Declaration and my Initial Supplemental Declaration remain unchanged. Further, as detailed in this Second Supplement Declaration, my opinion is that the Revised Substitute Claims set forth in Patent Owner's RMTA are unpatentable based on one or more of the following Grounds:

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

325. I have been informed that the '178 Patent claims priority to a provisional application filed June 23, 2011, that Petitioner treats as the earliest effective filing date of each revised substitute claim for the purposes of analysis herein, and that each prior art reference applied herein qualifies as prior art to each revised substitute claim even if Patent Owner could establish entitlement to the earliest effective filing date, based on at least the dates shown below:

| Reference | Filed | Published | Issued |
|---|---|---|---|
| Peterka | 10/26/2001 | 11/21/2002 | |
| Suzuki | | 06/10/2004 | |
| Bocharov | 03/16/2009 | 09/16/2010 | |
| Peterka308 | 08/22/2007 | 10/30/2008 | |
| Chen | | 5/12/2004 | |
| Traw | 04/13/2004 | | 06/24/2008 |

326. Additionally, based on my review of the file history, I note that none of the above references were cited or applied in a rejection during the original prosecution of the '178 Patent.

## II. PERSONAL AND PROFESSIONAL BACKGROUND

327. My professional experience, qualifications, experience testifying as an expert, and compensation are set forth in my Original Declaration (EX-1003, Orig. Decl., ¶¶ 1, 3-20) and my previously submitted *curriculum vitae* (EX-1004).

328. I also base this Second Supplemental Declaration on my personal knowledge, including my education, training, research, and professional experience.

## III. MATERIALS REVIEWED AND CONSIDERED

329. In reaching the conclusions described in this Second Supplemental Declaration, in addition to the documents identified in my Original Declaration (EX-1003, Orig. Decl., ¶ 21), I have considered the documents and materials cited herein, including:

| 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") |
| 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, *available at* 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 | *Apple Inc. v. Ericsson AB*, IPR2022-00618, Paper 2 (Feb. 25, 2022) |
| 1027 | *Apple Inc. v. Ericsson AB*, IPR2022-00618, Paper 9 (July 8, 2022) |
| 1028 | *Apple Inc. v. Ericsson AB*, IPR2022-00618, Paper 11 (Sept. 1, 2022) |
| 1029 | *Apple Inc. v. Ericsson AB*, IPR2022-00618, Paper 13 (Nov. 28, 2022) |
| 1030 | *Apple Inc. v. Ericsson AB*, IPR2022-00618, Paper 14 (Nov. 28, 2022) |
| 1031 | *Apple Inc. v. Ericsson AB*, IPR2022-00618, Paper 17 (Dec. 30, 2022) |
| 1032 | *In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same*, Inv. No. 337-TA-1376, Order No. 25 (Mar. 13, 2024) |
| 1033 | *In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same*, Inv. No. 337-TA-1376, Complaint, Exhibit 24 (October 12, 2023) |
| 1034 | *Telefonaktiebolaget LM Ericsson et al. v. Lenovo*, 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*, available at* https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf. |
| 1036 | *In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same*, Inv. No. 337-TA-1376, Final Initial Determination (Nov. 15, 2024) |
| 1037 | *In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same*, 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 *Pro Hac Vice* |
| 1039 | Declaration of Elizabeth A. DiMarco in Support of Admission *Pro Hac Vice* |
| 1040 | Deposition Transcript of John Villasenor |
| 1042 | U.S. Patent No. 7,392,381 ("Traw") |

| | |
|---|---|
| 1043 | USPTO Memorandum Re: PTAB Consideration of Prior Findings of Fact and Conclusions of Law (September 16, 2025) |
| 1048 | U.S. Patent App. Pub. No. 2008/0279387 ("Gassoway") |
| 1049 | U.S. Patent App. Pub. No. 2006/0236096 ("Pelton") |

330. I confirm that the statements made in my Original Declaration (EX-1003), my Initial Supplemental Declaration (EX-1041), and in my deposition testimony in this proceeding on May 29, 2025 (EX-2011) remain true to the best of my knowledge, and I continue to rely on the opinions expressed therein.

## IV. MY UNDERSTANDING OF PATENT LAW

331. The legal standards for patent invalidity that I have been informed about and used to render my unpatentability analysis are set forth in my Original Declaration (EX-1003, Orig. Decl., ¶¶ 22-34).

332. I have been informed that a Patent Owner may not amend or add a new claim that would introduce a new matter. I understand that new matter is subject matter that a person of ordinary skill in the art ("POSITA") would have understood not to have been disclosed in the original application.

## V. BACKGROUND

333. As explained in my Original Declaration (EX-1003, Orig. Decl., ¶ 35), the '178 Patent (EX-1001) relates to "Web-based delivery of files over the public Internet, referred to as over-the-top (OTT) delivery," and "encryption key rotation for live streaming media." '178 Patent, 1:15-23. The '178 Patent describes a server that streams segments of encrypted media content to a client. '178 Patent, 1:38-42,

1:63-65. The ’178 Patent explains that different segments in a media stream may be encrypted with different content encryption keys (“CEKs”). ’178 Patent, 1:45-65, 2:62-3:8. The ’178 Patent describes the client communicating with a license server to pre-fetch CEKs ahead of key rotation boundaries in the media stream, and then applying a retrieved key to decrypt a corresponding segment of the media stream. ’178 Patent, 11:3-25, 11:38-62. “The transitioning between use of different keys is also referred to” in the ’178 Patent “as key ‘rotation.’” ’178 Patent, 1:63-65.

334. A summary of relevant portions from the prosecution history of the ’178 Patent is set forth in my Original Declaration (EX-1003, Orig. Decl., ¶ 36).

335. As noted above, Patent Owner has proposed Revised Substitute Claims 21-37, as set forth in Patent Owner’s RMTA.

## VI. PERSON OF ORDINARY SKILL IN THE ART

336. In my opinion, the level of skill of the POSITA applicable to the Revised Substitute Claims is the same as that identified in my Original Declaration (EX-1003, Orig. Decl., ¶¶ 38-42) in connection with the Challenged Claims. In evaluating the obviousness of the Revised Substitute Claims, I have considered this same level of ordinary skill in the art.

## VII. CLAIM INTERPRETATION

337. As explained in my Original Declaration (EX-1003, Orig. Decl., ¶ 43), I understand that determining whether a claimed invention is novel and non-obvious

requires comparing the prior art to the claim. In accordance with the standards for interpreting patent claims terms discussed in Section IV above, I have interpreted the terms in the Revised Substitute Claims in accordance with their ordinary and customary meaning as understood by a POSITA in the context of the '178 Patent (including the descriptions in the specification) and its prosecution history.

## VIII. PRIOR-ART REFERENCES

338. A summary of the prior-art references discussed in Petitioner's Opposition to Patent Owner's Revised MTA is set forth in my Initial Supplemental Declaration (EX-1041, ¶¶ 243-252 (discussing Peterka), 253-256 (discussing Traw)).

## IX. THE REVISED SUBSTITUTE CLAIMS ARE UNPATENTABLE

339. I have been asked to provide my opinion concerning whether Revised Substitute Claims 21-37 of the '178 Patent are anticipated or would have been obvious to a POSITA in light of the prior-art references identified in Petitioner's Opposition to Patent Owner's RMTA. For the reasons explained below, it is my opinion that each of the Revised Substitute Claims would have been obvious.

340. A table summarizing the Grounds demonstrating unpatentability, including the references and relevant claims, is provided below. Peterka and Traw were described in my Initial Supplemental Declaration (EX-1041, ¶¶ 243-252

(discussing Peterka), 253-256 (discussing Traw)). The remaining references were described in my Original Declaration.

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

### A. Ground 6A: Peterka in view of Traw Renders Revised Substitute Claims 21-26, 29-30, 33-35, and 37 Obvious

341. As discussed below, Peterka-Traw renders obvious Revised Substitute Claims 21-26, 29-30, 33-35, and 37.

#### 1. Peterka-Traw

342. As discussed in my Initial Supplemental Declaration (EX-1041, ¶¶ 262-269), a POSITA would have had numerous reasons to modify Peterka's security mechanisms (*id.*, ¶¶ 243-252) to incorporate Traw's key revocation techniques (*id.*, ¶¶ 253-256) and would have reasonably expected success in doing so.

#### 2. Claim-by-Claim Analysis

##### a. Revised Substitute Claim 21

343. For the reasons explained below, Peterka-Traw renders substitute claim 21 obvious. Peterka-Traw maintains Peterka's system and most of its features. Therefore, much of my analysis from Ground 1 based on Peterka in my Original

Declaration is applicable to the Revised Substitute Claims. Specifically, the revised substitute claim limitations that are unchanged from original claim 1 are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶¶ 74-124. The limitations amended, changed, or added in Revised Substitute Claim 21 are obvious over Peterka-Traw as detailed below. Thus, I conclude that Revised Substitute Claim 21 is unpatentable.

**i. [21.P]**

344. Revised substitute limitation [21.P] is identical to Patent Owner's initial substitute limitation [21.P]. Revised substitute limitation [21.P] adds "for-over-the-top [('OTT')] media delivery." As explained in the Original Declaration, Peterka teaches rotation of keys in OTT streaming. *See* Peterka, [0004] ("[A] server can multicast a movie across the internet to client computers."), [0015] ("FIG. 1 is a block diagram of an embodiment of a content distribution system such as those used for multicasting program content over the internet."), [0038] (describing an embodiment of the content distribution system that includes "a network such as the internet"), [0135] ("System 1900 shows a client server network comprised of at least one client 1908 coupled to a server such as origin content processor 1904 via a network 1916 such as the internet."), FIG. 1; EX-1003, Orig. Decl., ¶¶ 150, 178. Therefore, Peterka-Traw satisfies [21.P] for the same reasons Peterka satisfies [1Pre]. EX-1003, Orig. Decl., ¶ 74.

**ii. [21.1]**

345. There are no amendments to [21.1]. Peterka-Traw satisfies [21.1] for the same reasons Peterka satisfies [1A]. EX-1003, Orig. Decl., ¶¶ 75-81.

**iii. [21.2]**

346. Revised substitute limitation [21.2] adds the requirement that the CEK identifiers are "each assigned to an associated content encryption key" and that the CEK identifiers are "uniquely identifying each associated content encryption key from every other content encryption key for the entire duration of a media playback." [21.2] also adds that the media playback "correspond[s] to the media playback request response." Peterka-Traw satisfies this limitation.

347. The '178 Patent specification (EX-1001) does not require any specific type of "assigning." Thus, the '178 Patent leaves to a POSITA the details of how "identifiers" are "assigned." For example, the '178 Patent describes key identifiers "selected based on" other data like "a segment number of the prepared content." EX-1001, 3:34-36; *see also id.*, 4:8-10 ("In another embodiment, the content encryption key identifiers are selected based on a number of the prepared content."), 6:1-4 ("In another embodiment, the content encryption key identifiers are based off of segment numbers, as produced by the packager 104 during segmentation."), 6:17-19 ("In another embodiment, the content encryption key identifiers are based off of segment numbers, as produced by the packager 104 during segmentation.").

348. Peterka discloses a sequence number or timestamp delivered to a client along with a CEK in an ECM/EMM. Peterka, [0121] (describing "a sequence number or a time stamp" in key-distribution ECMs "to protect against replay attacks"). Consistent with the '178 Patent (*see* above ¶ 347), a POSITA would have understood that Peterka's sequence number or timestamp is a unique CEK identifier that identifies the specific key in the ECM/EMM.

349. A POSITA further understood that Peterka's sequence number or timestamp, e.g., by virtue of being part of the key's ECM/EMM, was "assigned to an associated content encryption key" to the same extent that limitation is disclosed in the '178 Patent specification, which, as discussed above ¶ 347, leaves to the POSITA the details of how "identifiers" are "assigned."

350. Alternatively, "assign[ing]" an identifier "to an associated content encryption key" would have been obvious. A POSITA would have been motivated to implement Peterka's client to receive and use an assigned key identifier to identify the content key parsed from an ECM in view of Peterka's teachings—including, for example, Peterka's FIG. 7B, which expressly shows delivery of content keys with unique designations assigned to specific CEKs: $CK_0$, $CK_1$, $CK_2$. Peterka's FIG. 7B is reproduced below:

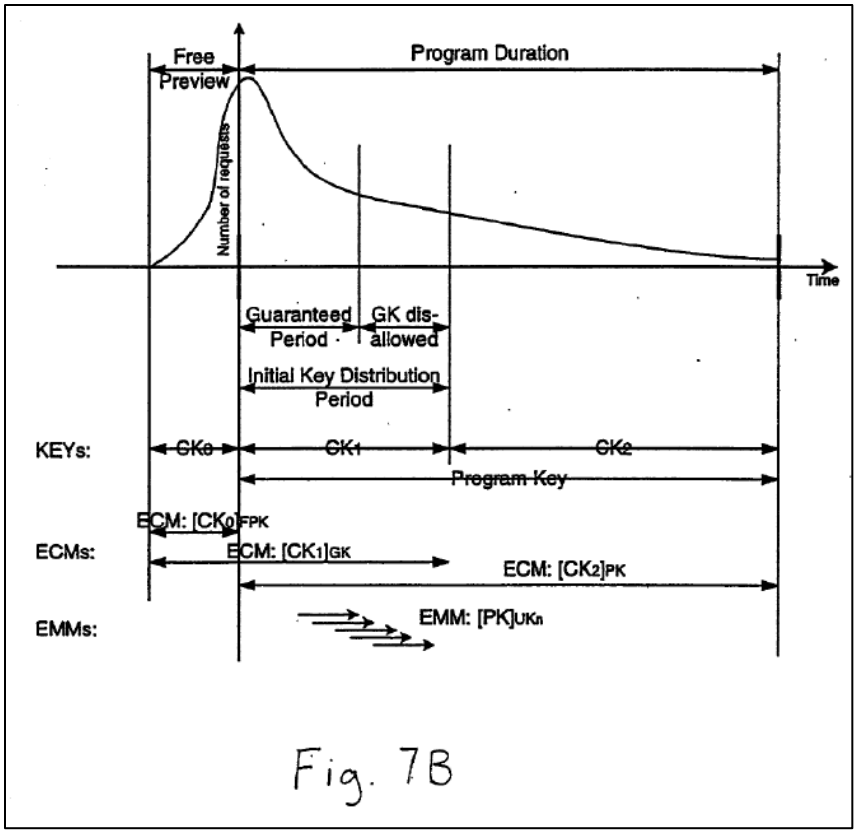



Fig. 7B

A POSITA would also have been motivated to implement Peterka's client to receive and use an assigned key identifier in view of Traw's teaching of the usefulness of assigned "key IDs" for targeted key revocations. Traw, 3:32-46. Assigned identifiers would have been particularly useful in scenarios where a single key (*see* Traw, 3:35, 4:45) that had already been distributed to multiple clients—e.g., with each client having respectively received the key in a separate ECM/EMM, per Peterka's teachings (*e.g.*, Peterka, [0121], FIG. 7B)—needed to be identified by the Peterka-Traw system for a targeted revocation due to, e.g., compromise. In addition, it was a well-known and well-documented key management technique to assign identifiers (e.g., key numbers) to CEKs to distinguish keys. This is described, e.g., in the Suzuki

(EX-1006) and Pestoni (EX-1012) references. Suzuki, [0013], [0016], [0030]-[0031], [0043]-[0048], [0080]-[0084], FIG. 5; Pestoni, 12:16-35; *see also* EX-1003, Orig. Decl., ¶¶93-96. POSITAs would have recognized the need to differentiate between keys, in systems like Peterka-Traw—where multiple keys are used. POSITAs would have further recognized that assigning CEK identifiers to differentiate keys would have been nothing more than implementing known methods (assigned CEK identifiers) to known systems (Peterka-Traw's key rotation with revocation system) to achieve predictable results (a key management scheme allowing Peterka-Traw's system to distinguish between keys).

351. POSITAs would have also reasonably expected success implementing assigned key identifiers in Peterka-Traw because this was a well-known, conventional option for implementing key identifiers. *See* Suzuki, [0013], [0016], [0030]-[0031], [0043]-[0048], FIG. 5; Pestoni, 12:16-35; *see also* EX-1003, Orig. Decl., ¶¶93-96. Moreover, Peterka expressly contemplates handling data that is key-specific, e.g., Peterka's key-specific key expiration times. Peterka, [0105], [0121] (describing an ECM/EMM field for "time remaining in the lifetime of the key").

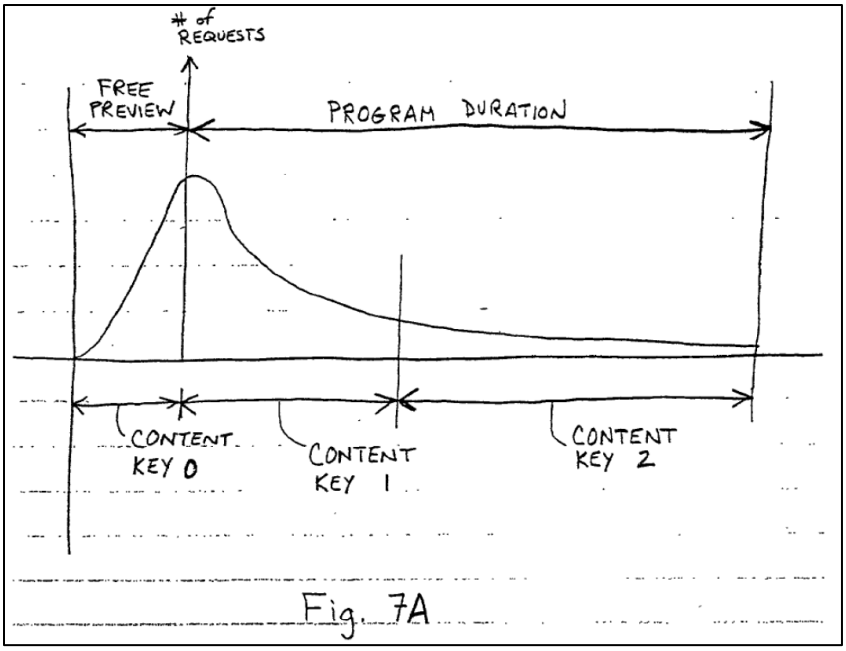
352. To the extent that Patent Owner argues that Peterka-Traw does not meet Patent Owner's new "assigned" requirement, it is expressly demonstrated as being obvious in view of the prior art discussed below in Section IX.B.

353. Because Peterka's "sequence number" or "timestamp" is specifically included "***to protect against replay attacks***" during media playback (Peterka, [0121]), POSITAs would also have understood that each sequence number/timestamp "uniquely identif[ies] each" ECM/EMM (and the "[CEK]" within it) "from every other" ECM/EMM and corresponding "[CEK] ***for the entire duration of a media playback***" as recited in [21.2]. *See, e.g.,* Peterka, FIG. 7B (expressly disclosing such a scenario).

354. A POSITA would also have had reason (and would have been motivated) to ensure uniqueness of key identifiers "for the entire duration of the media playback." As explained in my Original Declaration, POSITAs would have been motivated to implement Peterka's client to use key identifiers to differentiate between keys (and reasonably expected success) in view of Peterka itself and other references describing key management in multi-key environments. EX-1003, Orig. Decl., ¶¶ 94-96 (citing Suzuki, [0013], [0016], [0030]-[0031], [0043]-[0048], [0080]-[0084], FIG. 5; Pestoni, 12:16-35).

355. Further, consistent with the testimony I provided in my Original Declaration and at my deposition, POSITAs would have had reason to ensure that 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.*, Wechselberger Tr. (EX-2011), 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 systems"); EX-1003, Orig. Decl., ¶ 94. This is again confirmed by Peterka FIG. 7B, which illustrates such a scenario and shows content key identifiers—$CK_0$, $CK_1$, $CK_2$—that are unique for the entire program's duration. Peterka, FIG. 7B; *see also id.*, FIG. 7A, [0092] (FIG. 7A "illustrate[s] an example where only two keys are required to decrypt the remainder of the program"). FIGs. 7A and 7B of Peterka are reproduced below:



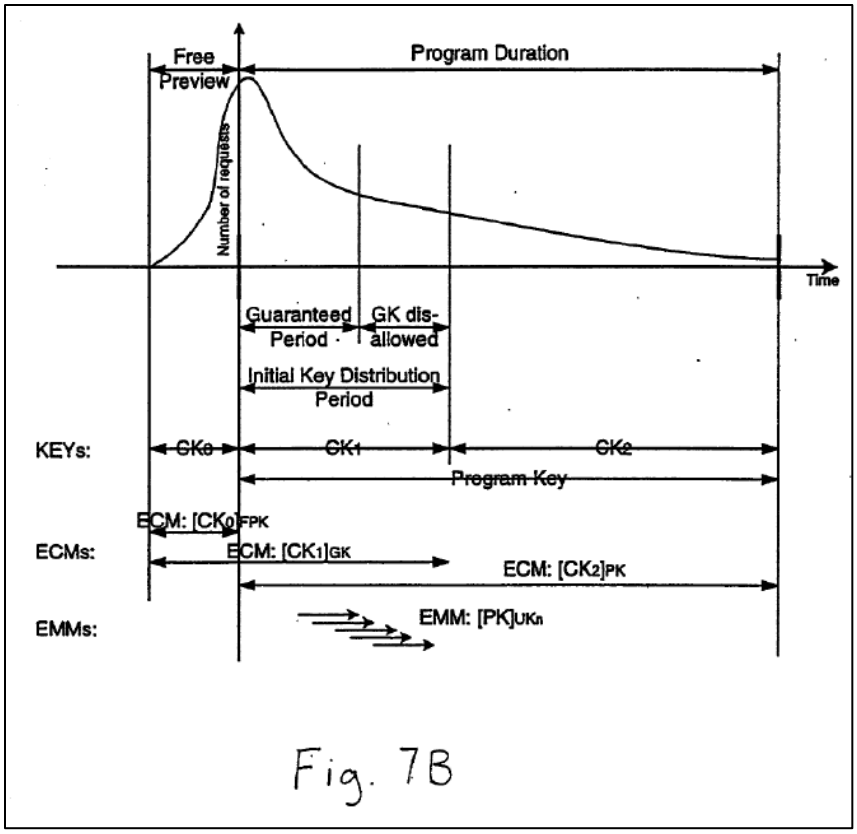



Fig. 7B

356. POSITAs would have reasonably expected success using identifiers sufficiently unique to distinguish between CKs over the entire duration of media playback given Peterka's teachings—Peterka, [0092] (describing FIG. 7A which shows "the distribution of content keys 0, 1, and 2"), 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. *E.g.,* Pestoni, 12:4-35 ("[T]he decryption key may protect a key box 420 that includes multiple decryption keys, each of which may protect a corresponding one of segments 440*a-c* ***of the encrypted content item associated with the content license***."), FIG. 4. FIG. 4 of Pestoni is reproduced below:

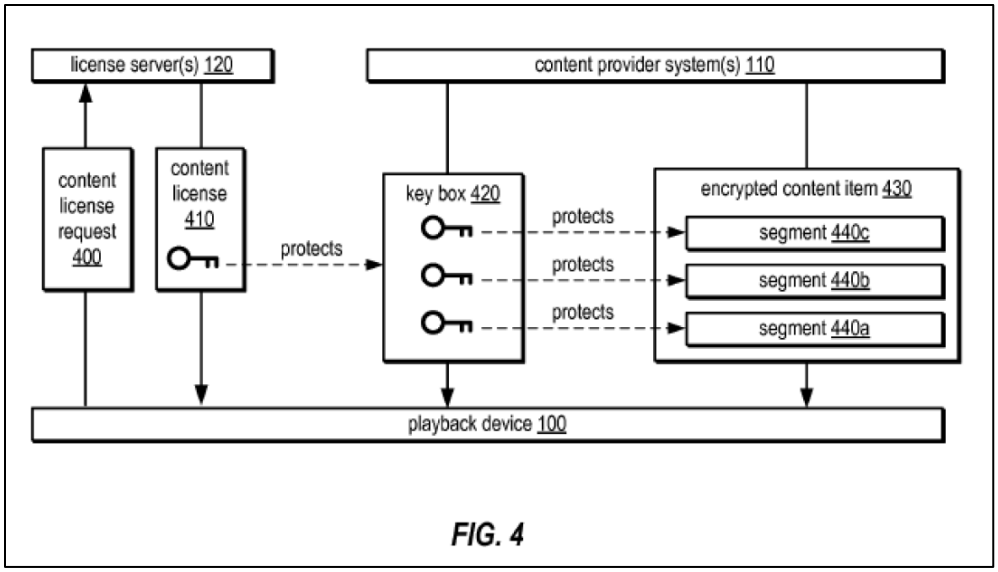



FIG. 4

357. POSITAs also would have understood that Peterka's "media playback ***correspond[s] to*** the media playback request response" as recited in [21.2], because, as I discussed in my Original Declaration, the CKs that Peterka's client receives when it first requests/negotiates access to a specific piece of media content are unsurprisingly used to decrypt and play back the specific piece of media content the client sought access to in the first place. *E.g.,* EX-1003, Orig. Decl., ¶ 50 (discussing Peterka's use of "content keys" to play back accessed media content that was encrypted), ¶¶ 75-77 (discussing Peterka's "media playback request" and "playback request response," and citing, e.g., Peterka, [0080]-[0082], [0091]-[0092], [0141]-[0143], FIGs. 7A-7B, 20A-20B), ¶¶ 85-87 (discussing Peterka's content keys ("CKs"), which are used to encrypt/decrypt the content that Peterka's client requested), ¶ 102 (discussing additional detail regarding Peterka's retrieval of

"content" corresponding to the CKs received in Peterka's "playback request response").

**iv. [21.3]**

358. There are no amendments to [21.3]. Peterka-Traw satisfies [21.3] for the same reasons Peterka satisfies [1C]. EX-1003, Orig. Decl., ¶¶ 102-110.

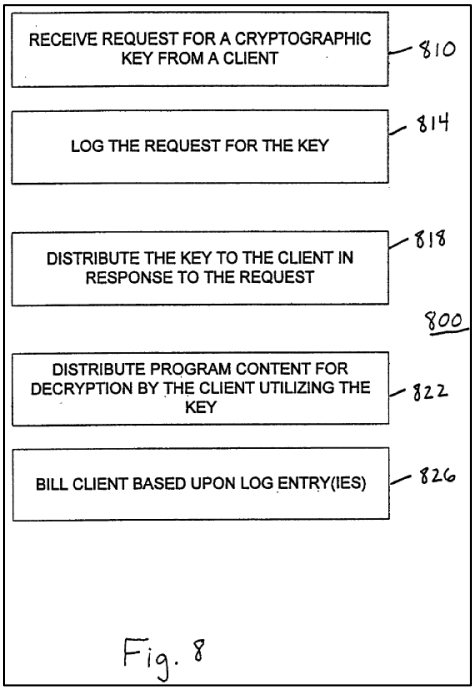
**v. [21.3A]**

359. [21.3A] adds the requirement "applying a first key for content decryption, said first key having a first expiration time defining a time-based [CEK] rotation boundary." Peterka-Traw satisfies this limitation.

360. Peterka discloses applying a first key for decrypting content. Peterka, [0106] ("decryption by the client" occurs "by utilizing the cryptographic key that was requested"), [0116] ("[T]he content key is utilized for decrypting the program content throughout the course of the distribution of the program content.…"); *see also id.*, [0090] ("keys for decrypting the encrypted portion of the program"), [0092] ("keys are required to decrypt…the program content"), [0108] ("the program content is distributed for decryption by the client utilizing the transmitted key").

361. Peterka also describes periodically rotating keys "at regular intervals." Peterka, [0110]; *see also id.*, [0082] ("The client will monitor the expiration time for each pay period and request a new set of keys from the caching server."). Peterka further describes that an ECM/EMM that carries a key to a client includes a field

indicating "the time remaining in the lifetime of the key" being delivered in the ECM/EMM. Peterka, [0121]; *see also id.*, [0106] ("[T]he key and its expiration time are distributed to the client…."), [0105] ("Under the pull model, each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions"), FIG. 8. FIG. 8 of Peterka is reproduced below:




362. Thus, a POSITA would have understood each key "expiration time" to define a "time-based [CEK] rotation boundary" for applying that key for decryption, after which a new key must be applied for decryption. Therefore, Peterka-Traw's client applies a first key for content decryption having a first expiration time that defines a time-based CEK rotation boundary.

**vi. [21.4]**

363. [21.4] adds the requirement of detecting "a notification, the notification including a notification-based [CEK] rotation boundary" wherein "the notification requires expiration of said first [CEK] earlier than said time-based [CEK] rotation boundary for said first key" and "after said notification-based [CEK] rotation boundary for said first key." Peterka-Traw satisfies this limitation.

364. Traw teaches revoking a key for security reasons before that key would ordinarily be rotated. Traw, 3:17-19 ("The revocation frequency may be changed depending on circumstances (e.g., if there exists more hacker activity, perform revocation more frequently)."), 5:29-31 ("As part of the renewal process, the device manufacturer may include new keys"), 5:35-39 ("Depending on market and suspected piracy conditions, or other events, the device manufacturer may increase or decrease the frequency of renewal. In one embodiment, the device manufacturer may have a renewal ready at all times for 'emergency' communication to the devices."), 6:12-21 ("the renewal may be performed at an earliest possible time before expiration of keys"), 6:39-57 ("[A]dditional flexibility regarding criteria for non-scheduled revocation is also possible….[R]enewal may be required on a more expedited basis than the regular periodic renewal."). And Traw also teaches notifying client devices of such revocations. *Id.*, 4:62-65 ("In yet another embodiment, the revocation data may be sent to the broadcaster for inclusion in a

broadcast transmission to devices. When a device receives the revocation data in broadcast content, the device processes the data."), 5:63-65 ("In one embodiment, generation of revocation data may trigger transmission of messages to users and/or devices announcing that renewal and/or revocation will be performed.").

365. As described above in [21.3A], in Peterka-Traw, keys would ordinarily be rotated based on the time-based CEK rotation boundary. Peterka, [0105] ("Under the pull model, each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions"), [0110] ("[T]he server can issue new keys at regular intervals to the active participants so as to prevent the removed client from decrypting further content."), [0121] (describing that an ECM/EMM that carries a key to a client includes a field indicating "the time remaining in the lifetime of the key" being delivered in the ECM/EMM).

366. In Peterka-Traw, notifications of these unscheduled key revocations are transmitted to (and detected by) the client using Peterka's key change signaling methods, as I discussed in my Initial Supplemental Declaration (EX-1041), Section IX.A.1. Peterka, [0116]-[0120] ("A signaling method can be used to indicate the implementation of a new key."). A POSITA would understand that the notification is a notification to stop using the current CEK and is thus a notification-based CEK rotation boundary. Peterka-Traw's client thus detects a notification-based CEK

rotation boundary where the notification requires early expiration of the first CEK earlier than the time-based CEK rotation boundary for the first key and after the notification-based CEK rotation boundary for the first key.

**vii. [21.5]**

367. [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 said time-based content encryption key rotation boundary for said first key to retrieve a second [CEK] to be used after ~~a~~ the notification-based [CEK] rotation boundary for said first key and before said time-based [CEK] rotation boundary for said first key is reached." Peterka-Traw satisfies this limitation.

368. A system that obtained a second CEK, applied that second CEK ***before*** the claimed content encryption key rotation boundary (in the revised substitute claim, the "time-based" boundary), and discarded that second CEK at or before the boundary (*i.e.*, did not apply it ***after*** the time-based boundary) would meet the requirements of this revised substitute claim yet ***would not*** meet the requirements of the original claim. A POSITA thus would have understood that applying a second CEK ***before*** a (e.g., the "time-based") key rotation boundary ***materially differs from*** applying a second CEK ***after*** that same key rotation boundary.

369. 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]

("Under the pull model, each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions.").

370. As explained above in [21.3A], POSITAs would have understood that the current key is set to expire (in other words, the key rotates) at the time-based CEK rotation boundary.

371. As explained above, Traw teaches unscheduled key revocations. Traw, 3:17-19 ("The revocation frequency may be changed depending on circumstances (e.g., if there exists more hacker activity, perform revocation more frequently)."), 5:29-31 ("As part of the renewal process, the device manufacturer may include new keys"), 5:35-39 ("Depending on market and suspected piracy conditions, or other events, the device manufacturer may increase or decrease the frequency of renewal. In one embodiment, the device manufacturer may have a renewal ready at all times for 'emergency' communication to the devices."), 6:12-21 ("the renewal may be performed at an earliest possible time before expiration of keys"), 6:39-57 ("[A]dditional flexibility regarding criteria for non-scheduled revocation is also possible….[R]enewal may be required on a more expedited basis than the regular periodic renewal."); *see also id.*, ("In yet another embodiment, the revocation data may be sent to the broadcaster for inclusion in a broadcast transmission to devices. When a device receives the revocation data in broadcast content, the device

processes the data."), 5:63-65 ("In one embodiment, generation of revocation data may trigger transmission of messages to users and/or devices announcing that renewal and/or revocation will be performed.").

372. And as explained in my Initial Supplemental Declaration (EX-1041), Section IX.A.1, Peterka teaches key change signaling methods that a POSITA would have had reason to use to signal to a client that keys have been revoked (and thus need renewal). Peterka, [0116]-[0120] ("A signaling method can be used to indicate the implementation of a new key.").

373. Therefore, a POSITA would have been motivated to implement Peterka-Traw such that when the client detects one of the unscheduled key revocations 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, so that it can be used before the current (compromised) key is set to expire (i.e., before the current key's original expiration time), in order to minimize the impact of the ensuing service interruption, as Peterka teaches. Peterka, [0105] ("Under the pull model, each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as ***to avoid service interruptions***."). A POSITA would have reasonably expected success with such an implementation, because reducing the amount of time that the client does not have the correct key to apply to

an encrypted content stream would enable the client to reduce the duration of any compromise-caused service interruption, which Peterka seeks to avoid (Peterka, [0105]). Such a request would satisfy revised substitute limitation [21.5].

374. Patent Owner's argument that neither Peterka nor Traw teach a client requesting a key in response to receiving notice that a key must be changed (RMTA, 16-17) is incorrect. As an initial matter, that argument is inconsistent with Peterka's teachings. Peterka teaches that under the pull key distribution model, "the responsibility of determining when a new key is required" is "passed to the client" (Peterka, [0106]) and "each client requests a new key and is individually responded to by the key distribution server" (Peterka, [0110]). Based on Peterka's teachings, POSITAs understood that "in response to" ***any*** scenario where Peterka's client determines a new key is required to decrypt content, the client request a new key. This includes scenarios such as the one I described for my modification in view of Traw—where Peterka's client determines that it does not have a required key due to notice of a key revocation.

375. Patent Owner's argument is also inconsistent with Traw's teachings. Traw discloses "requir[ing]" content protection implementations to be "renewable… ***in the event*** of revocation"—in other words, in response to a revocation—which Traw says can be "achieved by an on-line download of… a new content protection implementation." Traw, 2:43-64. As I discussed above in ¶¶ 364 and 371 (and in my

Initial Supplemental Declaration), one of the revocation events that Traw teaches is a revocation due to a compromised key or security breach. *See also* my discussion below in ¶ 396, citing Traw, 1:65-2:2, 2:15-19, 3:65-66, 4:37-39, 5:5-39, FIG. 2.[1]

376. Traw's disclosure of having keys be renewable via a "download" "***in the event***" of revocation is perfectly consistent with the basic, unremarkable concept of a client requesting a new key in response to notice that a key has been revoked—which was well-known in the client-server context. This was taught, for example, in the Gassoway (EX-1048) and Pelton (EX-1049) references. *E.g.*, EX-1048 ("Gassoway"), [0017] ("In step 106, a client makes a request of the server using the deprecated key. The server does not process the request; instead, the server sends a response to the client indicating that the client's key has been deprecated. This response may include instructions for obtaining the new replacement key. The instructions may be in the form of a link to a location where the new key is located, or a link to a site for downloading the new key."), [0018] ("In step 108 the client then automatically obtains the new key according to the instructions set forth in step 106. In step 110 the client then resubmits its server request using the new key. The client should then destroy the deprecated key and continue using the new key."), FIG. 1. FIG. 1 of Gassoway is reproduced below:

[1] For clarity that Traw's content protection implementations and renewals thereof may be directed to both software and keys, *see, e.g.*, Traw at claim 1.

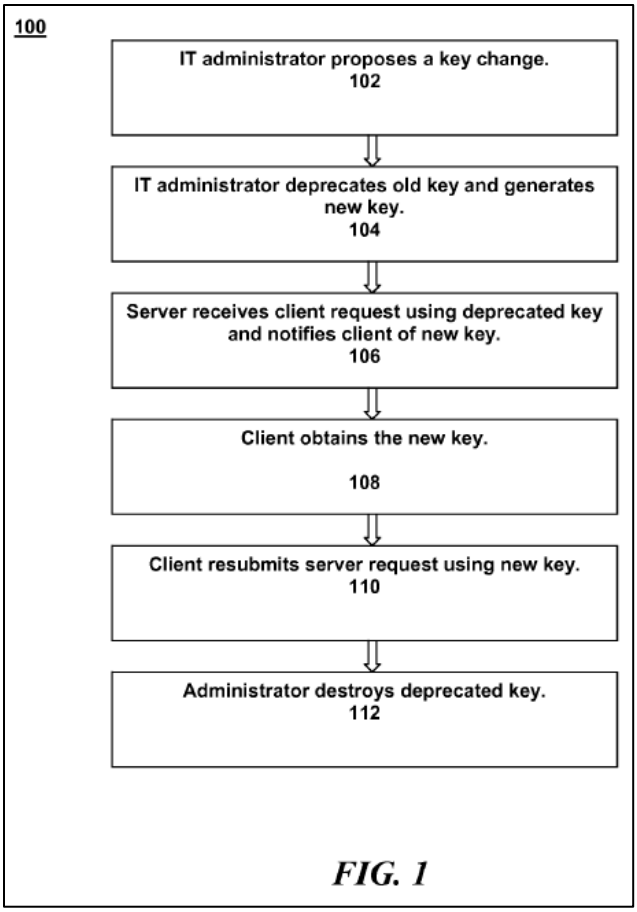



*FIG. 1*

*See also* EX-1049 ("Pelton"), [0147]-[0155] ("Various embodiments of the central key management system 10 are typically configurable to provide any or ***all of the following functions***:… Allowing ***key deletion, revocation, suspension*** and/or reissue of specific subject keys… Presenting configuration options for ***key request***, key maintenance, regular status, ***notification, and alerts*** for each subject…."). Pelton's reference to a system that supports functionality for revoking keys, notifications/alerts, ***and*** key requests confirms that key management systems where clients issue key requests in response to a key revocation were well-known.

377. Such teachings confirm that a POSITA would have found it desirable to implement Peterka-Traw, as I explained above in ¶ 373, to request a key in response to receiving notice that a key must be changed, in order to minimize service interruptions described in Peterka. Peterka, [0105] ("actively requests new keys before the current keys expire so as to avoid service interruptions").

**viii. [21.6]**

378. [21.6] changes the requirement from original claim 1 of applying the second key for content decryption "after the key rotation boundary" to applying the second key for content decryption after the "notification-based [CEK] rotation boundary for said first key" and "***before*** said time-based content encryption key rotation boundary for said first key is reached." Peterka-Traw satisfies this limitation.

379. To minimize "service interruptions" (Peterka, [0105]), a POSITA would have been motivated to implement Peterka-Traw such that when the client receives the second (replacement) key that was requested as a result of Traw's unscheduled key revocation (Traw, 3:17-19, 5:35-39, 6:12-21, 6:39-57; *see also id.*, 4:63-65, 5:63-65), the client promptly applies the second (replacement) key for decryption, before the current (compromised key) is set to expire (i.e., before the current key's original expiration time as taught by Peterka), thereby allowing the client to resume consuming content. *See* my discussion above in Section

IX.A.2.a.vii, for limitation [21.5], including my discussion of these portions of Traw, at ¶ 371; *see also* Peterka, [0106] (disclosing that "decryption by the client" occurs "by utilizing the cryptographic key that was requested" prior to the previous key's expiration), [0116] ("[T]he content key is utilized for decrypting the program content throughout the course of the distribution of the program content.… [W]hen a new content key is implemented, the implementation will be signaled to the clients so that the clients can begin utilizing the new content key with which they have been provided"); EX-1003, Orig. Decl., ¶ 124 (discussing that Peterka discloses applying the new key it requested—in other words, the second key for content decryption).

**b. Revised Substitute Claim 22**

380. Revised Substitute Claim 22 mirrors original dependent claim 2. *See* RMTA, Claims Appendix, ii. Unchanged claim limitations are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶ 125.

381. Revised Substitute Claim 22 adds the requirement that the CEK expiration time for the second CEK is "equal to the remaining lifespan of said first expiration time at the time said first [CEK] was expired." The amended limitation is obvious over Peterka-Traw as detailed below.

382. POSITAs 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. All three options would have been obvious to try.

383. Moreover, POSITAs had multiple reasons to try setting the CEK expiration time for the second CEK to be equal to the time remaining for the expiration previously set for the prior CEK (i.e., option #2 above).

384. ***First***, a POSITA would have been motivated to minimize the need to adjust any existing time variables in the system (at the client or server) that are associated with the first upcoming key rotation. Because the expiration time of the first (compromised) CEK was already known to both the client and server, setting the content key encryption time for the second CEK to be equal to the time remaining for the first CEK would have minimized such variable adjustment.

385. ***Second***, using the expiration time of the first key would have helped avoid forcing the system to adjust already-staged key rotation boundaries for remaining segments. This is because adjusting the expiration time of the second CEK such that it was not the same time as the first CEK would have required changing already-staged key rotation boundaries that are tied to future media segments, including interstitial segments like ads, previews, promotions etc. that were common in multicast content distribution systems. *E.g.*, Peterka, [0122] (describing FIG. 7B which illustrates a ***free preview*** period and associated keys tied to that period), FIG. 7B; *see also* Peterka308, [0024] (discussing an embodiment

where the DRM component generates a unique CEK for each segment during the recording), [0029] ("Each time that the DRM component 204 is asked to derive a new CEK and to set CCI [(control copy information)] values for protected outputs, the DRM component 204 selects the next consecutive CCI element."), [0032] (describing the process of utilizing encrypted segments); Chen [0034]-[0044] (describing FIG. 2C which illustrates an encoding scheme that uses markers to delimit crypto intervals in the stream), FIGs. 2A-2C. FIGs. 2A-2C of Chen are reproduced below:

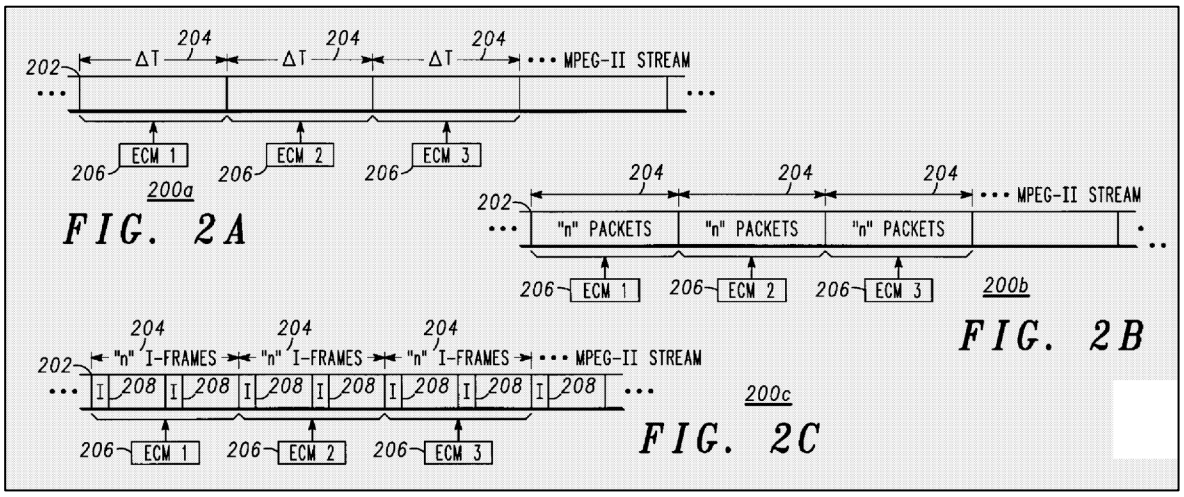


FIG. 2A

FIG. 2B

FIG. 2C

386. Further, given Traw's disclosure that its revocation can target a single key—Traw, 3:35 (describing revocation "may specify…***a single key ID***"), 4:44-45 ("The revocation data may comprise ***one*** or more revoked keys.")—a POSITA would have reasonably expected success revoking a single key and replacing it, leaving all other variables alone.

### c. Revised Substitute Claim 23

387. Revised Substitute Claim 23 mirrors original dependent claim 3. *See* RMTA, Claims Appendix, ii. Unchanged claim limitations are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶¶ 126-134.

388. Revised Substitute Claim 23 adds the requirement that the second CEK's expiration time is "equal to the first expiration time plus the remaining lifespan of said first expiration time at the time said first [CEK] was expired." RMTA, Claims Appendix, ii. The amended limitation is obvious over Peterka-Traw as detailed below. This limitation describes a scenario that falls within option #3 described above for Revised Substitute Claim 22: expiration for the second (replacement) CEK ***after*** the expiration of the first (compromised) key.

389. As noted above for Revised Substitute Claim 22, setting the expiration time for the second (replacement) CEK to occur ***after*** the expiration of the first (compromised) CEK was one of three obvious-to-try options.

390. POSITAs would have understood that setting the second CEK to both be applied ***before*** the first (compromised) key expires (see my discussion above in Section IX.A.2.a.viii, for limitation [21.6]) and then expire ***after*** the first CEK would have expired 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. In view of this issue—clients that had a compromised key and an upcoming key that was not used to encrypt any segment—POSITAs would have been motivated to set the CEK expiration time for the second CEK to be equal to the remaining lifespan for the pre-existing expiration set for the first CEK plus the fixed expiration (period duration) originally assigned for the first CEK. This would have given the Peterka-Traw 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 to be applied to the next media segment. Peterka, [0080] (noting the issue of "a large load on the caching server on the segment boundaries"). Additionally, using the second (replacement) CEK instead of the now-defunct key for the next segment would have provided some additional security, as it accounts for the possibility that the defunct key was also compromised along with the immediately preceding, original (compromised) key. Finally, this implementation would have avoided disrupting the encryption/decryption of future media segments, by desirably allowing POSITAs to avoid adjusting already-staged key rotation boundaries tied to future media segments. Peterka, [0122], FIG. 7B; *see also supra* ¶ 385 (citing Peterka308, [0024], [0029], [0032]; Chen [0034]-[0044], FIGs. 2A-2C).

391. POSITAs would have reasonably expected success with such an implementation because it would have allowed using a single unscheduled key rotation to cover two (previous) key rotation periods, giving servers more time to resume regular key distribution processes.

**d. Revised Substitute Claims 24-26 and 29**

392. There are no separate amendments in Revised Substitute Claims 24-26 and 29. Peterka-Traw satisfies Revised Substitute Claims 24-26 and 29 for the same reasons Peterka satisfies original claims 4-6 and 10. EX-1003, Orig. Decl., ¶¶ 135-153 (discussing claims 4-6 and 10 as obvious over Peterka).

**e. Revised Substitute Claim 30**

393. Revised Substitute Claim 30 mirrors original dependent claim 12. *See* RMTA, Claims Appendix, iv. Unchanged claim limitations are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶¶ 154-155.

394. Revised Substitute Claim 30 adds the requirement that the "retrieved content is divided into content segments, and said second [CEK] is applied to decrypt the same content segment for which the first [CEK] was used" and "notification-based expiration of the first [CEK] is for security reasons." *See* RMTA, Claims Appendix, iv. The amended limitation is obvious over Peterka-Traw as detailed below.

395. Peterka discloses content divided into segments encrypted (and decrypted) with a different key. Peterka, [0080]-[0082] (describing a "server" that "may divide the content into pay segments and assign segment keys to them": "All consumer computers would negotiate a key for each segment in order to keep track of how many segments they watched."), [0091]-[0101] (describing FIG. 7A, which shows a program that is divided and encrypted with a series of "content key[s]" and describing one way of dividing a program into "purchasable segments"), [0106], [0116] (discussing "the key distribution system [where] the content key is utilized for decrypting the program content throughout the course of the distribution of the program content."), [0121]-[0125] (describing FIG. 7B, which also shows a program that is divided and encrypted with a series of "content key[s]"), FIGs. 7A-7B.

396. In Peterka-Traw, Peterka's system is modified to include a mechanism to address security attacks, in view of the teachings in Traw, to revoke and require replacement of a key before it is otherwise set to expire (i.e., before the key's original expiration time as taught by Peterka). As shown above, the second CEK is used to decrypt content that was originally slated to be encrypted by the first (compromised) CEK, and the early expiration of the first (compromised) CEK is for security reasons. Traw, 1:65-2:2 ("An embodiment of the present invention is a system wherein revocation of cryptographic keys is used in combination with periodic renewal of compliant content protection implementations in a way that dramatically improves

the security of the overall content protection system."), 2:15-19 ("Embodiments of the present invention are applicable to security applications, but are described herein in term of their use in a system for protecting content…against unauthorized access, copying or distribution."), 3:65-66 (describing revocation of keys "reactively in response to an attack"), 4:37-39 ("The key generation facility determines when revocation of selected keys should occur. This may happen when it becomes known that some keys have been compromised."), 5:5-39 (describing FIG. 2 "illustrating forced renewal of a content protection implementation" and "[d]epending on market and suspected piracy conditions, or other events, the device manufacturer may increase or decrease the frequency of renewal. In one embodiment, the device manufacturer may have a renewal ready at all times for 'emergency' communication to the devices."), FIG. 2. Peterka-Traw thus meets the new requirements that "retrieved content is divided into content segments, and said second [CEK] is applied to decrypt the same content segment for which the first [CEK] was used" and "notification-based expiration of the first [CEK] is for security reasons," as claimed in Revised Substitute Claim 30.

**f. Revised Substitute Claims 33-35 and 37**

397. Revised Substitute Claim 33 mirrors original independent claim 16 in the same way that Revised Substitute Claim 21 amends claim 1. RMTA, Claims Appendix, i-ii, iv-v. Peterka-Traw maintains Peterka's system and most of its

features. Therefore, much of my analysis from Ground 1 based on Peterka in my Original Declaration is applicable to the Revised Substitute Claims. Specifically, the revised substitute claim limitations that are unchanged from original claim 16 are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶¶ 156-159. The limitations amended, changed, or added in Revised Substitute Claim 33 are obvious over Peterka-Traw as explained in the table below. Peterka-Traw's computerized device satisfies Revised Substitute Claims 33-35 and 37 for the same reasons described above for proposed Revised Substitute Claims 21-26 and 29-30.

| Proposed System Claim | Corresponding Proposed Method Claim | Section |
|---|---|---|
| [33.P] | [21.P] | § IX.A.2.a.i |
| [33.1] | - | EX-1003, Orig. Decl., ¶ 157 |
| [33.2] | [21.1] | § IX.A.2.a.ii |
| [33.3] | [21.2] | § IX.A.2.a.iii |
| [33.4] | [21.3] | § IX.A.2.a.iv |
| [33.4A] | [21.3A] | § IX.A.2.a.v |
| [33.5] | [21.4] | § IX.A.2.a.vi |
| [33.6] | [21.5] | § IX.A.2.a.vii |
| [33.7] | [21.6] | § IX.A.2.a.viii |
| [34] | [22] | § IX.A.2.b |
| [35] | [23] | § IX.A.2.c |
| [37] | [30] | § IX.A.2.e |

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

398. A POSITA would also have combined Traw with the original grounds set forth in the Petition (Grounds 2-5), for the same reasons discussed in my Initial Supplemental Declaration (EX-1041), Section IX.A.1. The addition of Traw would

not have changed the way the original combinations as set forth in my Original Declaration met the unchanged portions of the Revised Substitute Claims. Therefore, the resulting combinations (Peterka-Suzuki-Traw, Peterka-Suzuki-Bocharov-Traw, Peterka-Bocharov-Traw, Peterka-Bocharov-Peterka308-Chen-Traw) meet Revised Substitute Claims 21-26, 29-30, 33-35, and 37 for the same reasons discussed above in Section IX.A.2. Additionally, as summarized using the table below, those combinations ***also*** meet Revised Substitute Claims 27-28, 32, and 36 for the reasons I discussed in Grounds 2-5 of my Original Declaration, which had analyzed original claims 7-8, 14, and 19 and correspond to Revised Substitute Claims 27-28, 32, and 36 (without the proposed amendments).

| **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, **32**-35, 37 |
| 6D | Peterka, Suzuki, Bocharov, Traw | 21-26, 29-30, **32**-35, 37 |
| 6E | Peterka, Bocharov, Peterka308, Chen, Traw | **27-28**, **36** |

399. Further, to the extent that Patent Owner argues that Peterka-Traw does not disclose Patent Owner's new requirement in [21.2] that the CEK identifiers are "each assigned to an associated content encryption key," at least Grounds 6B and 6D, which incorporate Suzuki's "key number" teachings (Suzuki, [0030]) for identifying keys, meet the requirement that CEK identifiers are "each assigned to an associated content encryption key."

400. Grounds 6B and 6D implement Peterka's system to include Suzuki's "key number for identifying the key" (Suzuki, [0030]) to help the client keep track of keys, e.g., when determining which key to apply when decrypting a particular segment of content. Pet., 51-55 (citing Suzuki, [0030], [0043]-[0048], [0080], FIG. 2; Wechselberger, ¶¶161-172), 66-68 (citing Suzuki, [0030], [0043]-[0048], [0080], FIG. 2; Wechselberger, ¶¶201-207). As I discussed previously, a POSITA would have recognized the importance of using identifiers for keys (like Suzuki's key numbers) in multiple-key systems like Peterka's to help differentiate amongst keys and that ensuring those identifiers were unique values (like Suzuki's key numbers) helped ensure the system does not confuse keys. *See* Pet., 52-53; Wechselberger, ¶164. This would have been especially important and useful in the context of Peterka-Traw, for scenarios in which a ***single*** compromised key, that had already been sent to multiple clients, needs to be identified for revocation. Traw, 3:35, 4:45. POSITAs understood that in such scenarios, where each client respectively received the compromised key earlier in an ECM/EMM per Peterka's teachings (*e.g.,* Peterka, [0121], FIG. 7B), an assigned key identifier would be useful for the system to be able to identify the compromised key for all of the clients, when providing clients notice of the compromised key.

401. POSITAs understood that each key number in Peterka-Suzuki-Traw (Ground 6B) and Peterka-Suzuki-Bocharov-Traw (Ground 6D) was "assigned"

specifically to a key because the key number is information that is specifically associated with the key in order to allow the key to be identified. *See* Suzuki, [0013] (describing "key number" as "information for identifying the key").

402. Moreover, it would have been obvious to a POSITA to implement "key number for identifying the key" to be sufficiently "unique" to distinguish amongst keys "for the entire duration of a media playback," as claimed, for the same reasons discussed above ¶¶ 355-356 in the context of Peterka-Traw. A POSITA would have been motivated to ensure (and would have reasonably expected success ensuring) that 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 because the "need to identify" and "know which key to use when" is "fundamental" to "anybody who has worked with crypto-based content information distribution systems." EX-2011 (Wechselberger Tr.), 39:7-40:13. Peterka itself illustrates such a scenario. Peterka, [0092] ("At the bottom of FIG. 7A, the distribution of content keys 0, 1, and 2 is shown. Content key 0 is provided to the user in one embodiment for obtaining the free preview. Content keys 1 and 2 illustrate an example where only two keys are required to decrypt the remainder of the program content."), FIGs. 7A-7B. Further, a POSITA understood that it was common to use key IDs sufficiently unique to allow clients to keep track of keys required to playback a piece of content. Pestoni, 12:4-35 ("[T]he decryption key may protect a key box 420 that

includes multiple decryption keys, each of which may protect a corresponding one of segments 440*a-c* of the encrypted content item associated with the content license."), FIG. 4.

## X. CONCLUSION

403. For the foregoing reasons, as well as the reasons stated in my Original Declaration, it is my opinion that original claims 1-8, 10, 12, 14, and 16-20 of the '178 Patent are invalid as obvious. In addition, for the foregoing reasons, as well as the reasons stated in my Original Declaration and my Initial Supplemental Declaration, Revised Substitute Claims 21-37 of the '178 Patent are invalid as obvious.

404. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account any new information as it becomes available to me.

I understand and have been warned that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. § 1001). I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: December 4, 2025

Anthony Wechselberger

_____

Anthony J. Wechselberger