

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

IPR2025-00003
Patent No. 9,313,178

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

Google Exhibit 1041 Google v. Ericsson IPR2025-00003
--

TABLE OF CONTENTS

I.	SUMMARY OF OPINIONS.....	1
II.	PERSONAL AND PROFESSIONAL BACKGROUND	3
III.	MATERIALS REVIEWED AND CONSIDERED	3
IV.	MY UNDERSTANDING OF PATENT LAW	5
V.	BACKGROUND	7
VI.	PERSON OF ORDINARY SKILL IN THE ART	7
VII.	CLAIM INTERPRETATION	8
VIII.	PRIOR-ART REFERENCES.....	8
	A. Peterka	8
	B. Traw	16
IX.	THE SUBSTITUTE CLAIMS ARE UNPATENTABLE.....	20
	A. <u>Ground 6A</u> : Peterka in view of Traw Renders Substitute Claims 21- 26, 29-30, 33-35, and 37 Obvious	22
	1. Peterka-Traw	22
	2. Claim-by-Claim Analysis.....	28
	a. Substitute Claim 21	28
	i. [21.P].....	28
	ii. [21.1].....	29
	iii. [21.2].....	29
	iv. [21.3].....	33
	v. [21.4].....	33
	vi. [21.5].....	35
	vii. [21.6].....	38
	b. Substitute Claim 22	39
	c. Substitute Claim 23	41
	d. Substitute Claims 24-26 and 29	43
	e. Substitute Claim 30	43
	f. Substitute Claim 33-35 and 37	46

B. Additional Traw Combinations (Grounds 6B-6E).....	47
C. <u>Ground 7</u> : Substitute Claims 21-37 Are Indefinite	48
1. All claims: “the expiration time-based key rotation boundary previously provided for the content encryption key currently being used”	48
2. All claims: “for the duration of the media playback”	48
3. Claims 22-26 and 33-37: “second content key” in relation to “expiration times”	50
D. <u>Ground 8</u> : Substitute Claims 21-37 Claim Unpatentable Subject Matter.....	51
X. CONCLUSION.....	51

I, Anthony J. Wechselberger, declare:

224. 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 No. 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-1043.

225. Petitioner has asked that I consider certain new arguments raised by Patent Owner, Ericsson AB (“Patent Owner”) in a Motion to Amend (Paper 24, “MTA”) after I provided my Original Declaration. I submit this Supplemental Declaration to address arguments raised in Patent Owner’s MTA and to provide opinions relating to the unpatentability of Patent Owner’s proposed substitute claims 21-37 (“Substitute Claims”).

I. SUMMARY OF OPINIONS

226. My opinions set forth in my Original Declaration remain unchanged. Further, as detailed in this Supplemental Declaration, my opinion is that the Substitute Claims set forth in Patent Owner’s MTA are unpatentable based on one or more of the following Grounds:

Ground and Reference(s)		Claims
6A	Peterka, Traw (EX-1042)	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
7	Indefiniteness	21-37
8	Unpatentable Subject Matter	21-37

227. 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 substitute claim for the purposes of the analysis herein, and that each prior art reference applied herein qualifies as prior art to each 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

228. 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

229. 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).

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

III. MATERIALS REVIEWED AND CONSIDERED

231. In reaching the conclusions described in this 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, <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, available at 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
1042	U.S. Patent No. 7,392,381 (“Traw”)

232. I confirm that the statements made in my Original Declaration (EX-1003) and in my deposition testimony in this proceeding on May 29, 2025 (EX-1043) remain true to the best of my knowledge, and I continue to rely on the opinions expressed therein.

IV. MY UNDERSTANDING OF PATENT LAW

233. 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).

234. I understand that 35 U.S.C. § 101 describes the law regarding the subject matter eligible for patenting. In particular, 35 U.S.C. § 101 states that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements.” For the purposes of this declaration, my understanding of 35 U.S.C. § 101 is that patent protection is limited to a particular technological environment, and abstract ideas are not eligible for patent protection. Moreover, merely adding insignificant post solution activity and well-understood, routine, conventional activity do not render an abstract claim patent eligible.

235. I have been informed that a Patent Owner may not amend or add a new claim that would introduce 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.

236. I have also been informed that, in a Patent Office proceeding such as an *inter partes* review proceeding, a claim is indefinite when it contains words or phrases whose meaning is unclear to a POSITA. I have also been informed, that in a federal court proceeding, a claim is indefinite, when viewed in light of the specification and prosecution history, it fails to inform those skilled in the art about the scope of the invention with reasonable certainty.

V. BACKGROUND

237. As explained in my Original Declaration (EX-1003, Orig. Decl., ¶ 36), 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.

238. 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).

239. As noted above, Patent Owner has proposed substitute claims 21-37, as set forth in Patent Owner's MTA.

VI. PERSON OF ORDINARY SKILL IN THE ART

240. In my opinion, the level of the skill of the POSITA applicable to the 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 Substitute Claims, I have considered this same level of ordinary skill in the art.

VII. CLAIM INTERPRETATION

241. 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 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.

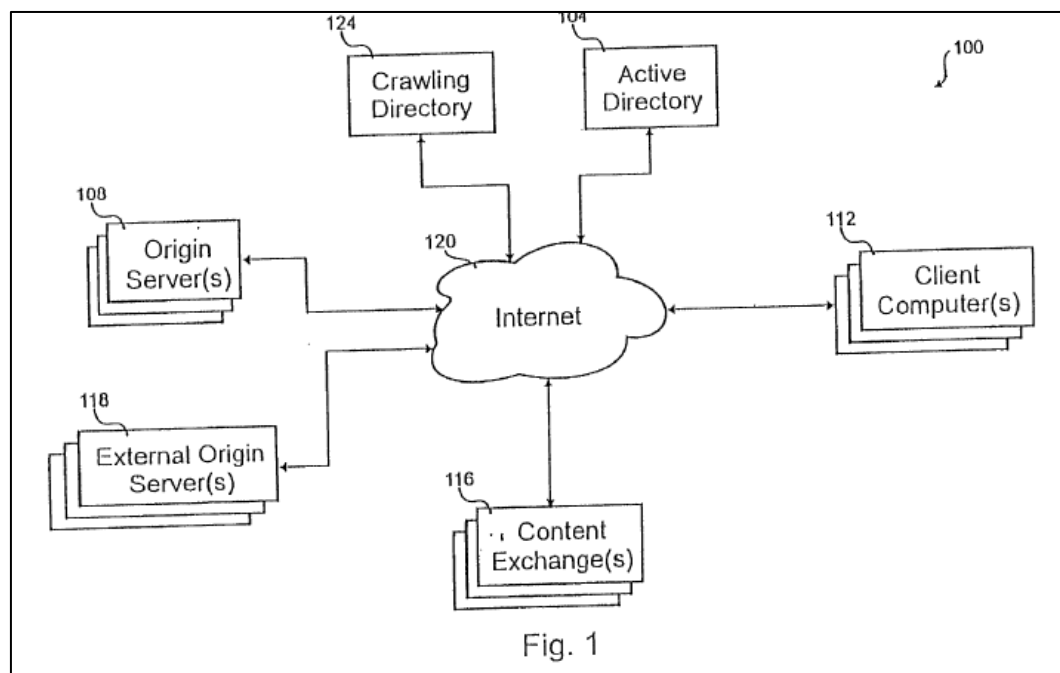
VIII. PRIOR-ART REFERENCES

242. As I did for my Original Declaration (EX-1003, Orig. Decl., ¶¶ 44-65), I briefly introduce in this Section below various prior-art references discussed in Petitioner's Opposition to Patent Owner's MTA.

A. Peterka

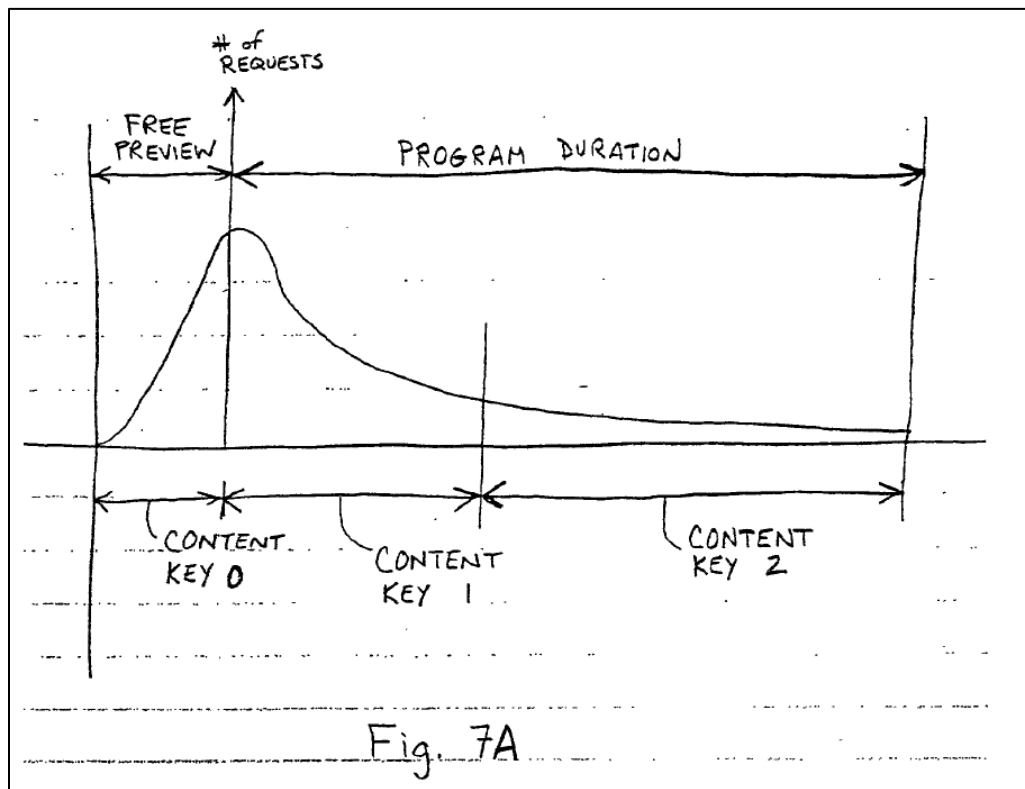
243. Peterka (EX-1005) is directed to a multimedia distribution system for securely delivering streaming media to authorized devices over a network. Peterka, Abstract (“[V]arious distribution methods can be accomplished using encryption keys to distribute program content.”), FIG. 1, [0038] (“Referring to FIG. 1, a block diagram of a content distribution system 100 is shown.... A particular client

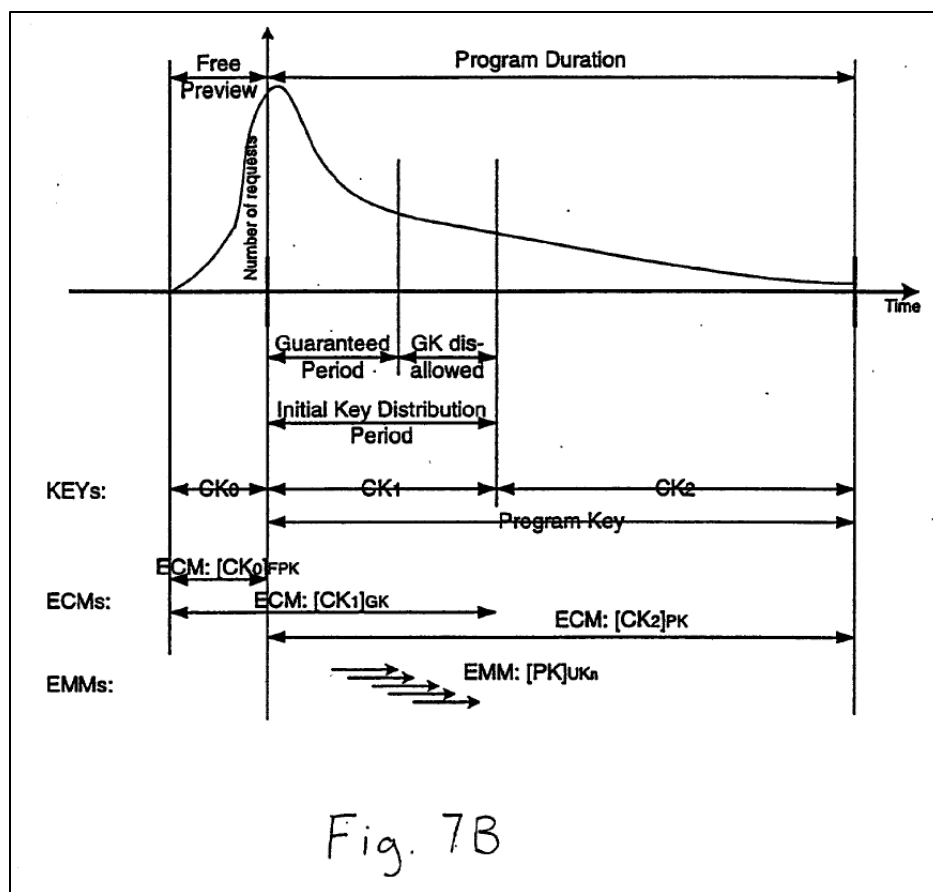
computer 112 is shown interacting with the active directory 104 to select a content object for downloading. The object can be played during download if it is a streaming media or can be stored for later display. The content object could be various types of information, such as audio, video, or data that is available to be downloaded from the network. Furthermore, it can be used for multicasting and/or unicasting.”), [0006]-[0012] (summarizing “a method of multicasting program material is provided by providing encrypted program material for distribution to a client”). FIG. 1 of Peterka is reproduced below:



244. Peterka teaches its “client” devices downloading streaming media from a content distribution system comprising servers. Peterka, [0038]. Peterka also teaches dividing content into “segments” that are each encrypted with a different key prior to streaming. 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.”), [0099]-[0101] (describing one way of dividing a program into “purchasable segments”), [0091]-[0093] (describing FIG. 7A, which shows a program that is divided and encrypted with a series of “content key[s]”), [0122]-[0125] (describing FIG. 7B, which also shows a program that is divided and encrypted with a series of “content key[s]”), FIGs. 7A-7B. Figures 7A and 7B of Peterka are reproduced below:





245. Peterka discloses servers distributing content to clients using various purchase mechanisms, including “pay-by-time (PBT)” —in which users pay for the time duration of content that is actually watched. Peterka, [0053] (“Pay-By-Time (PBT)—A purchase mechanism in which the client pays for the time duration of the content that was actually watched. The discrete time increments may have different durations for different programs or services.... Some sporting and music events are of this type.”). Users may pay for, *e.g.*, each media segment requested. Peterka, [0080] (“All consumer computers would negotiate a key for each segment in order to keep track of how many segments they watched.”), [0099] (describing one way

of implementing acquisition of keys for a program divided into “purchasable segments”).

246. Peterka teaches streaming encrypted media content segments to clients in packets, *e.g.*, Real-Time Transport Protocol (“RTP”) packets. Peterka, [0043]. Peterka teaches that the media content may be, for example, in the well-known MPEG-4 format. Peterka, [0119]. Peterka also teaches that the media content its system distributes may be “live content.” Peterka, [0058] (“Multicast—Multicast is similar to the existing TV broadcast. It delivers the same content to one or more consumers at the same time. This is usually scheduled and can be live content.”).

247. Peterka also teaches using content packets to signal key changes to clients. Peterka, [0116]-[0120] (teaching various ways to provide “key change” notifications, including, for example, in RTP packet headers). Note that Peterka’s disclosed “signaling methods” inform a client precisely when to start using a new key to decrypt received content, *regardless of how that key was obtained by the client*. Peterka’s *separate* teachings regarding obtaining keys (independent of Peterka’s signaling teachings) include several ways for a client to obtain a next key before it is needed for decryption. Peterka, [0105]-[0115]. For example, Peterka describes a “Push” model for key distribution (where a server keeps track of keys at each client and pushes keys as needed), a “Pull” model for key distribution (where a client keeps track of its keys and actively requests keys as needed), and a

combination “Push-Pull” model for key distribution (*e.g.*, where a server pushes keys to only those clients which have confirmed receipt of a previous key). Peterka, [0105] (describing the different models), [0106]-[0110] (pull model), [0111]-[0112] (push model), [0113]-[0115] (push-pull model). A POSITA would have understood that all of these methods for obtaining keys were compatible with Peterka’s signaling methods for informing clients *when* to change keys used for decryption. See my additional discussion in paragraphs 115-117 of my original declaration. For the purpose of this declaration, I focus my analysis on Peterka’s pull-model for key distribution—in which a client keeps track of its own keys and sends requests to a server to obtain keys as needed.

248. For each encrypted content segment, Peterka teaches a client obtaining the key that was used to encrypt the segment—*e.g.*, a content key (“CK”)—and applying that key to decrypt the segment before playing it back. Peterka, [0011] (“One embodiment allows providing a key and utilizing the key to accomplish the encrypting of a remaining portion of the program. In addition, one embodiment may allow the user to purchase the program content as well as provide the user with a key that is operable to decrypt the encrypted portion of the program.”), [0091]-[0093] (describing an implementation of FIG. 7A where clients obtain “[c]ontent keys” that “are required to decrypt” various portions of “program content.”), [0127] (explaining that “clients... utilize the content key to decrypt the encrypted program content”),

FIG. 7A. For embodiments where keys themselves are encrypted, Peterka teaches issuing (1) an encrypted version of a key that was used to encrypt a segment of media content and (2) at least one secondary key used to encrypt the key. Peterka, [0094]-[0104]. An authorized user's client applies the secondary key(s) to decrypt the encrypted key to obtain the content key, which is then used to decrypt content. *Id.*

249. Peterka teaches that each key, along with information about the key, is distributed to a client device in an Entitlement Control Message (“ECM”) or an Entitlement Management Message (“EMM”). Peterka, [0104], [0121]-[0125], FIG. 7B. While Peterka teaches generally that EMMs and ECMs perform different types of messaging, Peterka also discloses they can perform similar messaging. *See, e.g.*, Peterka, [0104] (“These [EMM] group-addressed multicast messages play the role of Entitlement Control Message (ECM) messages”), [0125] (“CK2 may be encrypted with the UK [(unique key)] and delivered in the form of an EMM directly to the client instead of the ECM form shown in the figure.”).

250. As discussed, in Peterka's “pull model” for obtaining keys, “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.” Peterka, [0105]-[0106], FIG. 8. To mitigate excessive server loads at media segment boundaries in such an embodiment—that is, an embodiment (as Peterka teaches) where clients actively request and negotiate keys for segments—the POSITA would have

understood Peterka to teach distributing *multiple* keys (*e.g.*, multiple ECMs) to a client (*e.g.*, for the current *and* next media segment) in response to such a request. Peterka, [0080] (when discussing what Peterka calls “a quasi-PBT approach” where “a caching server 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. This generates a large load on the caching server on the segment boundaries. This can be mitigated with a key management approach where each rabbit is given keys to the current as well as the next segment. This will give the caching server enough time to distribute the next segment keys during the current segment.”);¹ *see also* Peterka, [0130] (discussing FIG. 7B: “Any user that purchases the program content during the guaranteed period will receive the next necessary decryption key within the initial key distribution.”), FIG. 7B.

251. Peterka also discloses embodiments in which clients can adjust the quality (*e.g.*, bit rate) of the media its users view (for example, for an MPEG-4

¹ The use of the term “rabbit” in paragraph [0080] is a typographical error. Based on Peterka’s disclosures and the context that Peterka is describing in the surrounding text, a POSITA would have understood Peterka to be referring to “clients” receiving “keys to the current as well as the next segment.” *See* Peterka, [0078]-[0080].

format stream, per Peterka, [0119]) but does not specify the mechanism by which clients receive information that facilitates such adjustments—such as information regarding what quality encodings are available to stream. Peterka, [0054] (“Pay-By-Quality (PBQ)—Content may be offered at a different quality (i.e., bit rates), either as separate streams or as layered streams with each additional layer adding quality to the content. The client may report the highest bit rate it can consume and be offered to purchase the content at that quality or less. The server may also adjust the rate in real time based on the immediate state of the network.... The client may also adjust the bit rate perceived by the user, in accordance with user selection.”).

252. Based on Peterka’s disclosures and a POSITA’s background knowledge, a POSITA would have understood Peterka’s teachings about content being available at different network rates or quality levels (Peterka, [0054])—and users having the option to choose between various offered media qualities—would be implemented with Peterka’s various disclosed purchase mechanisms, including pay-by-time (Peterka, [0078]-[0082])—for example in an implementation where users are charged based on the time duration of content viewed, at a chosen quality/bit rate.

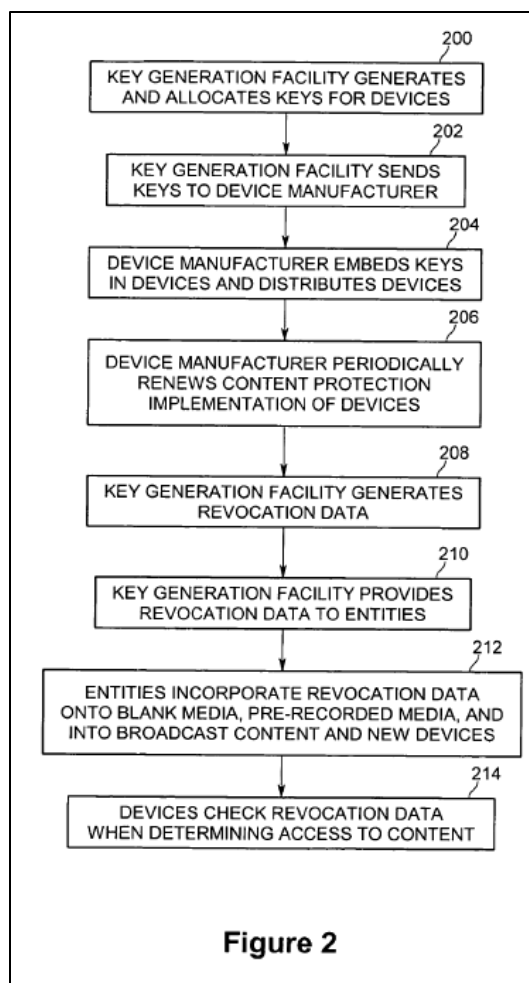
B. Traw

253. Traw (EX-1042) describes 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.*, 1:65-2:2 (key “revocation is also used to prevent access to content if the devices’ keys have been compromised”), 4:37-39 (“They key generation facility determines when revocation of selected keys should occur. This may happen when it becomes known that some keys have been compromised.”). Traw’s system thus “protect[s] content (such as audiovisual entertainment content) against unauthorized access, copying or distribution.” *Id.*, 2:15-19. Traw explicitly states that its system is “especially” suited for electronic devices that “include software for assisting in implementing content protection and wherein the software may be updated via a communication mechanism (such as... the Internet...)” *Id.*, 2:19-51.

254. Traw describes two types of key revocation in which current content keys are rotated or replaced: **(1)** periodic or planned key revocation (Traw, 5:15-17 (describing an embodiment where key “may also include an expiration date, such that the key may be scheduled to be revoked on a certain date or after a certain number of days has transpired”), 5:33-35 (“In one embodiment, the device manufacturer may perform the renewal periodically, according to any selected frequency.”), 6:10-12 (“[R]evocation data may be sent periodically in conjunction with the renewal scheme, instead of in response to a known compromise of one more keys.”)); **(2)** non-periodic or unplanned key revocation based on compromised keys, piracy or other security attacks, or emergency situations (Traw,

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.”), 5:5-7 (“FIG. 2 is a flow diagram illustrating forced renewal of a content protection implementation according to an embodiment of the present invention.”), 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.”), FIG. 2). FIG. 2 of Traw is reproduced below.



255. In my unpatentability analysis I draw from Traw’s disclosures directed to *key* updates (revocation or rotation). Traw’s teachings describe two renewal concepts: renewal of a device’s content protection implementation, and renewal or revocation of keys. Traw teaches that these operations need not be considered together, and does not teach that they happen in any specific or required sequence. *See* Traw, 6:58-62 (“Although the operations described herein may be described as a sequential process, some of the operations may in fact be performed in parallel or concurrently. In addition, in some embodiments the order of the operations may

be rearranged”); *see also id.*, 2:19-21 (“The security systems include means for revoking implementations, including ... content protection systems.”), 5:29-31 (“...as part of the renewal process, the device manufacturer may include new keys.”). Thus, POSITAs would understand that Traw’s teachings collectively address both the updating of content protection implementations and the updating of keys, and do not strictly constrain either to the exclusion of the other, in timing, frequency, sequencing—or, in the use of the terms renewal vs. revoke/revocation.

256. Traw describes “transmission of messages to users and/or devices announcing that... revocation will be performed.” Traw, 5:63-65.

IX. THE SUBSTITUTE CLAIMS ARE UNPATENTABLE

257. I have been asked to provide my opinion concerning whether 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 MTA, whether the claims are indefinite, and whether the claims are directed to unpatentable subject matter. For the reasons explained below, it is my opinion that each of the Substitute Claims would have been obvious, indefinite to a POSITA, and/or trying to claim unpatentable subject matter.

258. A table summarizing the additional Grounds demonstrating unpatentability, including the references and relevant claims, is provided below.

Peterka and Traw are described above in Section VIII. The remaining references were described in my Original Declaration.

Ground and Reference(s)		Substitute Claims
6A	Peterka, Traw (EX-1042)	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
7	Indefiniteness	21-37
8	Unpatentable Subject Matter	21-37

259. 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 substitute claim for the purposes of the analysis herein, and that Traw applied herein qualifies as prior art to each substitute claim even if Patent Owner could establish entitlement to the earliest effective filing date, on at least the bases shown below:

Reference	Filed	Published	Issued
Traw	04/13/2004		06/24/2008

260. Additionally, based on my review of the file history, I note that Traw was not cited or applied in a rejection during the original prosecution of the '178 Patent.

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

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

1. Peterka-Traw

262. A POSITA would have had numerous reasons to modify Peterka's security mechanisms (as I discussed above, in Section VIII.A) to incorporate Traw's key revocation techniques (as I discussed above, in Section VIII.B) and would have reasonably expected success in doing so.

263. Peterka and Traw are in the same field of art. Both describe systems that distribute secure content encrypted with content keys and changing/rotating those keys. *Compare* Traw, Abstract ("A system for proactive forced renewal of content protection implementation in devices includes a key generation facility to generate and allocate keys for the devices, and to generate revocation data corresponding to revoked keys in response to at least...a security compromise...and a device manufacturer to receive the keys from the key generation facility, to embed the keys in content protection implementations for the devices"), 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."), 2:56-60 ("Content protection

implementations are required in embodiments of this invention to be proactively renewed (i.e., replaced) by their implementer on a periodic basis, independent of whether revocation has occurred.”), 3:13-19 (discussing revocation of keys), 4:11-14 (“Devices 108, 110, to 112 use the keys embedded in their content protection implementations to decrypt and/or otherwise access the protected content broadcast by the broadcaster.”), *with* Peterka, [0116]-[0121] (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”), FIG. 14 (illustrating a flow chart for implementing a signaling method to indicate the implementation of a new key).

264. Both Peterka and Traw also teach providing content keys to clients for decryption. *Compare* Traw, 3:63-66 (describing FIG. 1, which is a diagram of a content protection system providing keys to clients for decryption), 4:11-14 (“Devices 108, 110, to 112 use the keys embedded in their content protection implementations to decrypt and/or otherwise access the protected content broadcast by the broadcaster.”), 5:5-19 (describing FIG. 2, which is a flow diagram illustrating forced renewal of keys for decryption), FIGs. 1-3, *with* Peterka, [0080] (describing “a key for each segment in order to keep track of how ma[n]y segments they watched”), [0105]-[0106] (describing models for distributing “the keys”), [0130] (describing FIG. 7B, which illustrates “the guaranteed time period...during which

the group key can be utilized to decrypt a content key which is encrypted program content”), 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 (“[R]evocation may entail distributing a list of key IDs to be revoked, where each revocation list entry may specify either a single key ID or a range...of key IDs.”), *with* Peterka, [0121] (“a sequence number of a time stamp to protect against replay attacks”).

265. Peterka and Traw also share common objectives to limit or prevent unauthorized access to content. *Compare* Peterka, [0135]-[0146] (describing “rules and conditions for providing content in a multicasting environment” to only authorized clients), *with* Traw, 2:15-19 (“Embodiments of the present invention are applicable to security applications in general, but are described herein in terms of their use in a system for ***protecting content...against unauthorized access***, copying or distribution.”).

266. Peterka recognizes that security attacks may be attempted and provides some security mechanisms to protect against them, *e.g.*, changing keys “at regular intervals” (Peterka, [0110]) (periodic key rotation) and “a time stamp” in key-distribution ECMs “to protect against replay attacks.” Peterka, [0105], [0121]. 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, as in prior systems.”). Traw *also* recognizes the benefits of “non-scheduled revocation,” 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).

267. Peterka leaves to the POSITA how to resolve unauthorized access to content after a security attack. *See* Peterka, [0110] (providing options for how to resolve unauthorized access to content in the event of a security attack). As I discussed above, in Section VIII.B, a POSITA understood that Traw teaches such details, describing that compromised keys should be revoked, including in systems with key rotation. Traw, 6:39-56 (describing the benefits of “non-scheduled revocation” including for keys that “have been compromised”). Thus, a POSITA understood that Traw’s teachings discussing security-driven key revocation complement and support Peterka’s goal of limiting media access to authorized users (Peterka, [0110])—a goal that Traw also shares (Traw, 6:39-57).

268. POSITAs thus would have been motivated to improve Peterka’s system in view of Traw by:

- **First**, providing a client a notification—using Peterka’s content packet “signaling methods” for key changes (Peterka, [0116]-[0120])—that a certain key requires early expiration, for example, because the key may have been compromised, in view of Traw. Traw, 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. In another embodiment, the revocation and renewal operations are transparent to the users.”), 3:34-35 (“where each revocation list entry may specify either a single key ID or a range”), 4:44-45 (“The revocation data may comprise one or more revoked keys.”), 4:62-65 (“[T]he 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.”).

- ***Second***, having the client obtain a replacement key using Peterka’s “pull” method (Peterka, [0105]-[0106]) when notified that the current key has been revoked before the originally-scheduled expiration of the compromised key, in view of Traw. Traw, 6:18-21 (“[R]enewal may be performed at an earliest possible time before expiration of keys, or at in a ‘just in time’ manner.”)); and
- ***Third***, 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] (“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.”).

This modified system—“Peterka-Traw”—would have maintained Peterka’s overall system (which uses content packet key change signals and the pull-method for acquiring new keys, as taught by Peterka) while beneficially improving security by including a mechanism to address security attacks—namely, revoking and requiring replacement of a compromised key before it is set to expire (as taught by Traw).

269. POSITAs would have reasonably expected success implementing Peterka-Traw. Traw teaches a straightforward way to address security compromises that is easily adaptable to Peterka’s system. Peterka, [0105]-[0106] (describing pull method for acquisition of new keys, which the POSITA would have understood could be used by clients to acquire new keys after receiving notification of compromised keys or other security breaches), [0116]-[0120] (describing content stream signaling of the need to use new keys, which the POSITA would have understood could be used to notify clients of a key compromise or other security breach), [0121] (describing “a sequence number or a time stamp” in key-distribution ECMs “to protect against replay attacks”), [0135]-[0138] (describing a system for providing content to authorized users in a multicasting environment).

2. Claim-by-Claim Analysis

a. Substitute Claim 21

270. 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 Substitute Claims. Specifically, the 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 substitute claim 21 are obvious over Peterka-Traw as detailed below. Thus, I conclude that substitute claim 21 is unpatentable.

i. [21.P]

271. 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]

272. 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]

273. Substitute limitation [21.2] adds the words “that uniquely identify each [CEK] from every other [CEK] for the duration of the media playback” after the term “content encryption key identifiers.” While there is no intrinsic support for this limitation (see my discussion in Section C.2), Peterka-Traw satisfies this requirement, as discussed below.

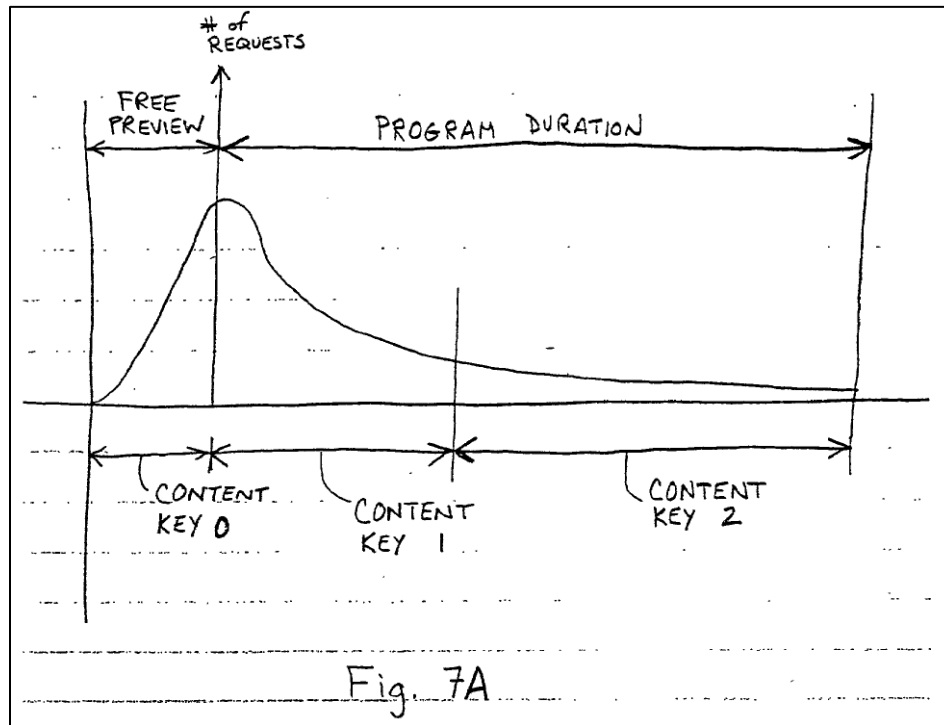
274. Peterka discloses a sequence number or timestamp delivered to a client along with a CEK in an ECM/EMM. Peterka, [0121] (describing “a sequence number or a time stamp” in key-distribution ECMs “to protect against replay attacks”). Thus, because Peterka’s “sequence number” or “timestamp” is specifically included “*to protect against replay attacks*” during media playback (Peterka, [0121]), POSITAs would 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 duration of the media playback” as recited in [21.2]. See, e.g., Peterka, FIG. 7B (expressly disclosing such

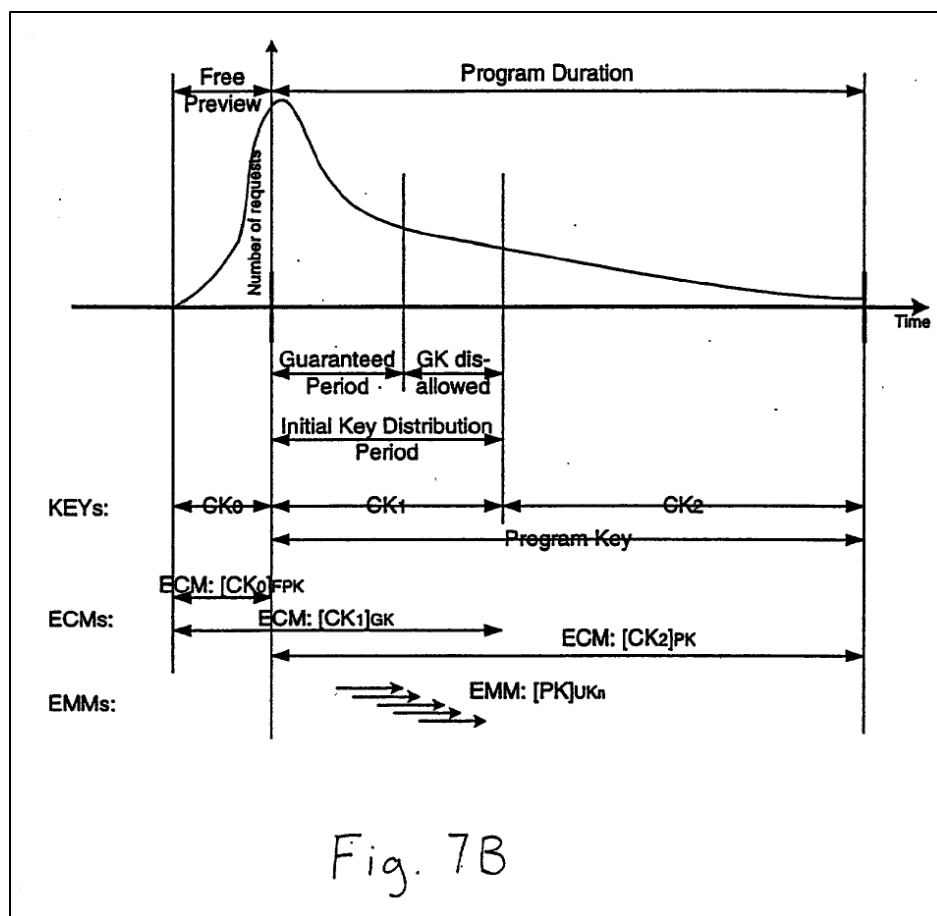
a scenario).

275. A POSITA would also have had reason (and would have been motivated) to ensure uniqueness of key identifiers “for the 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).

276. 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—CK0, CK1, CK2—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.

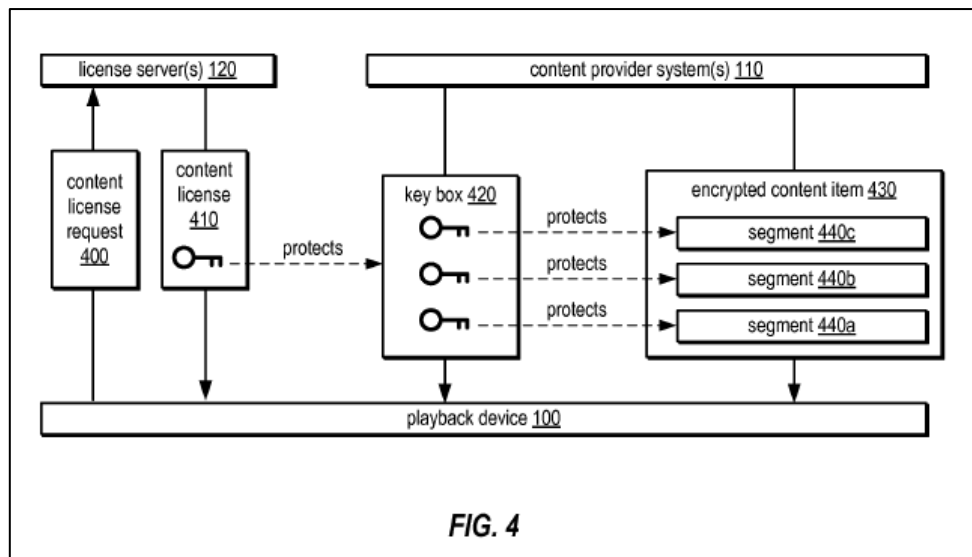
7A and 7B of Peterka are reproduced below:





277. POSITAs 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] (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 440a-c *of the encrypted content item associated with the content license.*”), FIG. 4. FIG. 4 of Pestoni is reproduced

below:



iv. [21.3]

278. 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. [21.4]

279. [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.” Peterka-Traw satisfies this limitation.

280. 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.”).

281. 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 above in Section IX.A.1. Peterka, [0116]-[0120] (“A signaling method can be used to indicate the implementation of a new key.”). Peterka-Traw’s client thus detects notification-based CEK rotation boundaries where a notification requires early expiration of the current CEK.

vi. [21.5]

282. [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 a~~ before said expiration time-based [CEK] rotation boundary for the [CEK] currently being used is reached.” 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. A POSITA thus would have understood that applying a second CEK *before* a key rotation boundary *materially differs from* applying a second CEK *after* a key rotation boundary. Further, as I discuss below in Section § IX.C.1, there is no antecedent basis for the purported “expiration time-based key rotation boundary.” To the extent this limitation is not indefinite, Peterka-Traw satisfies this clause, as discussed below.

283. 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.”).

284. 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.”).

285. And as explained above in 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.”).

286. 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, before the current (compromised) key is set to expire, 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 substitute limitation [21.5].

vii. [21.6]

287. [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.”

288. As I discuss below in Section IX.C.1, there is no antecedent basis for the purported “expiration time-based key rotation boundary.” To the extent this limitation is not indefinite, Peterka-Traw satisfies this clause.

289. 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, thereby allowing the client to resume consuming content. *See* my discussion above in Section IX.A.2.a.vi, for limitation [21.5], including my discussion of these portions of Traw, at ¶ 249; *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. Substitute Claim 22

290. Substitute claim 22 mirrors original dependent claim 2. *See* MTA, 16. Unchanged claim limitations are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶ 125.

291. Claim 22 adds the requirement that the content key encryption expiration time for the second CEK is “equal to the time remaining for the expiration previously set for the prior [CEK].” The amended limitation is obvious over Peterka-Traw as detailed below.

292. 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.

293. 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).

294. **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 prior (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 prior CEK would have minimized such variable adjustment.

295. **Second**, using the expiration time of the original 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 prior 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.

296. 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 compromise *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. Substitute Claim 23

297. Substitute claim 23 mirrors original dependent claim 3. *See* MTA, 16. Unchanged claim limitations are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶¶ 126-134.

298. Claim 23 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] *plus* the fixed expiration period duration originally assigned for the prior [CEK].” The amended limitation is obvious over Peterka-Traw as detailed below. This limitation describes a scenario that falls within option #3 described above for substitute claim 22: expiration for the second (replacement) CEK *after* the expiration of the prior (compromised) key.

299. As noted above for substitute claim 22, setting the expiration time for the second (replacement) CEK to occur *after* the expiration of the prior (compromised) CEK was one of three obvious-to-try options.

300. POSITAs would have understood that setting the second CEK to both be applied *before* the prior (compromised) key expires (*see* my discussion above in Section IX.A.2.a.vii, for limitation [21.6]) and then expire *after* the prior 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 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 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* ¶ 260 (citing Peterka308, [0024], [0029], [0032]; Chen [0034]-[0044], FIGs. 2A-2C).

301. 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. Substitute Claims 24-26 and 29

302. There are no separate amendments in substitute claims 24-26 and 29. Peterka-Traw satisfies 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. Substitute Claim 30

303. Substitute claim 30 mirrors original dependent claim 12. *See* MTA, 17-18. Unchanged claim limitations are obvious for the same reasons set forth in Ground 1 of my Original Declaration. EX-1003, Orig. Decl., ¶¶ 154-155.

304. Claim 30 adds the requirement that the “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.” The amended limitation is obvious over Peterka-Traw as detailed below.

305. 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.

306. 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 (or keys) before it is otherwise set to expire. As shown above, the second CEK is used to decrypt content that was originally slated to be encrypted

by the prior (compromised) CEK, and the early expiration of the prior (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 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,” as claimed in the substitute claim.

f. Substitute Claim 33-35 and 37

307. Substitute claim 33 mirrors original independent claim 16 in the same way that substitute claim 21 amends claim 1. MTA, 18-19. 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 Substitute Claims. Specifically, the 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., ¶¶ 156-158. The limitations amended, changed, or added in substitute claim 33 are obvious over Peterka-Traw as explained in the table below. Peterka-Traw's computerized device satisfies substitute claims 33-35 and 37 for the same reasons described above for proposed 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
[33.5]	[21.4]	§ IX.A.2.a.v
[33.6]	[21.5]	§ IX.A.2.a.vi
[33.7]	[21.6]	§ IX.A.2.a.vii
[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)

308. A POSITA would also have combined Traw with the original grounds set forth in the Petition (Grounds 2-5), for the same reasons discussed above in Section X.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 Substitute Claims. Therefore, the resulting combinations (Peterka-Suzuki-Traw, Peterka-Suzuki-Bocharov-Traw, Peterka-Bocharov-Traw, Peterka-Bocharov-Peterka308-Chen-Traw) meet substitute claims 21-26, 29-30, 33-35, and 37 for the same reasons discussed above in Section X.A.2. Additionally, as summarized using the table below, those combinations *also* meet 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 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, <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: Substitute Claims 21-37 Are Indefinite

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

309. Substitute limitations [21.5] and [33.7] lack proper antecedent basis for the phrase “the expiration time-based key rotation boundary previously provided.” 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.*” Therefore it is unclear toPOSITAs what “the expiration time-based key rotation boundary” is, when it is provided, and what it does.

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

310. Substitute claims 21/33 similarly lack proper antecedent basis for the phrase “[CEK] identifiers that uniquely identify each [CEK] from every other [CEK] for the duration of the media playback.” The claims never introduce any such concept before this limitation.

311. Moreover, the ’178 Application does not describe *the duration of the media playback* when discussing CEK identifiers. The ’178 Application instead states:

The changing of [CEKs] based on the fixed period of the live content is referred to herein as rotation. A history of individual [CEKs] and the order in which they were generated is maintained. Each [CEK] in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier.

EX-2007, ¶8. As can be seen above, there is no discussion of the “duration of media playback.” Moreover, there is no suggestion that the individual CEK “history” is tied to the duration of media playback.

312. The ’178 Application explicitly contemplates live streaming content that has uncertain duration, and states that: “For live streaming content with long or indefinite durations, use of a single encryption key for the entire duration increases the probability that the key may be compromised.” EX-2007, ¶2. The POSITA is given no specific information about what is meant by a “long duration” or an “entire duration,” other than stating that the duration may be “indefinite.” Likewise, the ’178 Application does not provide any other information regarding the scope of “the duration of the media playback” term. The term *media playback* is disclosed as something that is initiated, but never constrained to any specific duration, whether live or otherwise. *See, e.g.*, EX-2007, ¶5 (describing a client initiating a playback request), ¶8 (describing a client initiating playback of a stream).

313. Further, the ’178 Application does not describe the *duration* for which the uniqueness of any “identifier” must be maintained. POSITAs understood that how long a client maintains a “history” is at least partially determined by factors that are independent of the length of a media program that the client may ultimately stream (*e.g.*, available memory at the client, security settings associated with the client, etc.). Moreover, POSITAs understood that it was possible that the “history”

described in the '178 Application could—for example, for programs “with long or indefinite durations” (EX-2007, ¶2)—be *shorter* than the entire *duration of the media playback*. The little information that is disclosed regarding the CEK “history” in the '178 Application in my opinion fails to provide sufficient definiteness for “*the duration of the media playback*” term. Therefore, it is unclear to POSITAs what “for the duration of the media playback” means in the context of the substitute claims, and the specification provides no guidance.

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

314. The substitute claims add the term phrase “the content key expiration time for said second [CEK],” which lacks antecedent basis as explained below.

315. Substitute claims 22/33 require a CEK that was received in the playback request response to be replaced—after a notification to do so—by a “second” CEK, which is obtained through a separate request and response. *See* MTA, 16, 19.

316. Meanwhile, 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 relating to the CEK expiration times in the (original) playback request response’s content information.

317. The Patent Owner’s amendments thus conflate the two separate claimed requests/responses creating an unresolved ambiguity for a POSITA that cannot be reasonably understood.

D. Ground 8: Substitute Claims 21-37 Claim Unpatentable Subject Matter

318. Substitute claims 21-37 describe computer implementations of a very basic concept—the claims are directed to the abstract idea of using CEKs to encrypt and decrypt information (segments of media content) using a general-purpose computer. The substitute claims recite the use of generic, conventional computer technology without reciting any improvement in computer architecture or functionality.

X. CONCLUSION

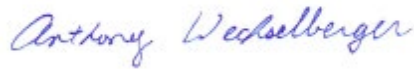
319. For the foregoing reasons, as well as the reasons stated in my Original Declaration, it is my opinion that original claims 1-8, 10, 12, 14, and 16-20 of the '178 Patent are invalid as obvious. In addition, for the foregoing reasons, substitute claims 21-37 of the '178 Patent are invalid under 35 U.S.C. § 103, 35 U.S.C. § 112, and/or 35 U.S.C. § 101.

320. 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 new information as it becomes available to me.

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: September 5, 2025



Anthony J. Wechselberger