Filed: May 7, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

SANDPIPER CDN, LLC,

Patent Owner.

Case IPR2025-00846
Patent No. 8,595,778

PETITION FOR *INTER PARTES REVIEW*
OF U.S. PATENT NO. 8,595,778

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

REGULATIONS

LIST OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 8,595,778 to Maloney ("'778 patent")
1002	Prosecution History of U.S. Application No. 12/604,678
1003	Declaration of Bill Lin ("Lin")
1004	Curriculum Vitae of Bill Lin
1005	U.S. Patent Publication No. 2003/0165241 to Fransdonk ("Fransdonk")
1006	U.S. Patent No. 6,718,328 to Norris ("Norris")
1007	U.S. Patent Publication No. 2007/0198839 to Carle et al. ("Carle")
1008	U.S. Patent Publication No. 2003/0221127 to Risan et al. ("Risan")
1009	U.S. Patent Publication No. 2006/0253399 to Chatani ("Chatani")
1010	U.S. Patent Publication No. 2004/0024688 to Bi et al. ("Bi")
1011	U.S. Patent Publication No. 2002/0112240 to Bacso et al. ("Bacso")
1012	Sandpiper's Preliminary Claim Chart, submitted in *Sandpiper CDN, LLC v. Google LLC*, No. 2:24-cv-03951 (C.D. Cal. May 10, 2024)
1013	U.S. Patent Publication No. 2009/0019469 to Foti et al. ("Foti")
1014	Balachander Krishnamurthy et al., On the Use and Performance of Content Distribution Networks, Proceedings of the 1st ACM SIGCOMM Workshop on Internet measurement, November 2001 ("Krishnamurthy")

Exhibit	Description
1015	Zhuoqing Morley Mao et al., A Precise and Efficient Evaluation of the Proximity between Web Clients and their Local DNS Servers, Proceedings of the 2002 USENIX Annual Technical Conference, June 2002 ("Mao")
1016	U.S. Patent Pub. No. 2002/0078233 to Biliris et al. ("Biliris")
1017	U.S. Patent No. 8,336,773 to Trimper et al. ("Trimper")

*All emphasis is added unless otherwise indicated.

I. Introduction

Petitioner requests that the Board institute review of claims 1-20 of U.S. Patent No. 8,595,778 (the "'778 patent") (Ex. 1001) and find those claims unpatentable.

The '778 patent claims computer-implemented methods for delivery of video content across a network. '778 patent, Abstract. Content delivery management systems and content delivery networks with the features of the '778 patent were known before its effective date. For example, using a subscription database to determine if a user is authorized to watch content—the purportedly novel feature of the claims—was disclosed in the prior art, including the prior art cited herein. Claims 1-20 are thus unpatentable.

II. Statement of Precise Relief Requested

Petitioner requests review under 35 U.S.C. § 311 of claims 1-20 of the '778 patent and their cancelation in view of the following:

Prior Art References	
Ref. 1:	Fransdonk (Ex. 1005), published September 4, 2003, and is prior art under 35 U.S.C. § 102(b).[1]
Ref. 2:	Norris, (Ex. 1006), issued on April 6, 2004, and is prior art under 35 U.S.C. § 102(b).

[1] Citations to 35 U.S.C. §§102, 103, and 112 are to the pre-AIA statutes.

Ref. 3:	Carle (Ex. 1007), published on August 23, 2007, and is prior art under 35 U.S.C. § 102(b).
Ref 4:	Foti (Ex. 1013), filed on July 11, 2007, is prior art under 35 U.S.C. § 102(e).

Grounds of Unpatentability	
1A	Claims 1, 4-12, and 14-20 are anticipated by Fransdonk under 35 U.S.C. § 102.
1B	Claims 1, 4-12, and 14-20 are rendered obvious by Fransdonk under 35 U.S.C. § 103.
2	Claims 2-3 and 13 are rendered obvious by Fransdonk in view of Norris under 35 U.S.C. § 103.
3	Claims 4-8 are rendered obvious by Fransdonk in view of Carle under 35 U.S.C. § 103.
4	Claims 9-12 are rendered obvious by Fransdonk in view of Foti under 35 U.S.C. § 103.
5	Claim 13 is rendered obvious by Fransdonk in view of Foti in further view of Norris under 35 U.S.C. § 103.

III. The ’778 Patent

A. Technology Overview

Content delivery networks (CDNs) are geographically dispersed servers for delivering content to end-users, usually on a national or global scale. Risan

(Ex. 1008), Abstract; Krishnamurthy (Ex. 1014), Abstract; Mao (Ex. 1015), Abstract; Biliris, (Ex. 1016), ¶[0003]. As both the prior art and the '778 patent recognize, the advent of the Internet increased the amount of information and content available for end users to consume. *See* Chatani (Ex. 1009), ¶[0003]; Bi (Ex. 1010), ¶¶[0004]-[0005]; *see also* '778 patent (Ex. 1001), 1:25-54. As one way of accommodating the large volume of information, CDNs reduced demand on origin servers by replicating content on CDN servers. Krishnamurthy, Abstract; Mao, Abstract; Biliris, ¶[0003]. Moreover, to control access to content on these servers, CDNs incorporated authentication means to verify end-user requests, including by verifying a user's metadata, verifying a user's geographic information, or by using database management calls. *See* Chatani, ¶¶[0021]-[0022]; Bi, ¶[0123]; Bacso (Ex. 1011), ¶¶[0040], [0084] [0087]; Lin, ¶43.

B. Summary of the '778 Patent

The '778 patent was filed on October 23, 2009, as U.S. Application 12/604,678 and claims priority to U.S. Provisional Application No. 61/113,941, filed November 12, 2008. '778 patent, cover.

The '778 patent discloses a system and methods for delivering content to multiple users across a network. '778 patent, Abstract. Figure 17 is representative. *See* Figure 17 below:

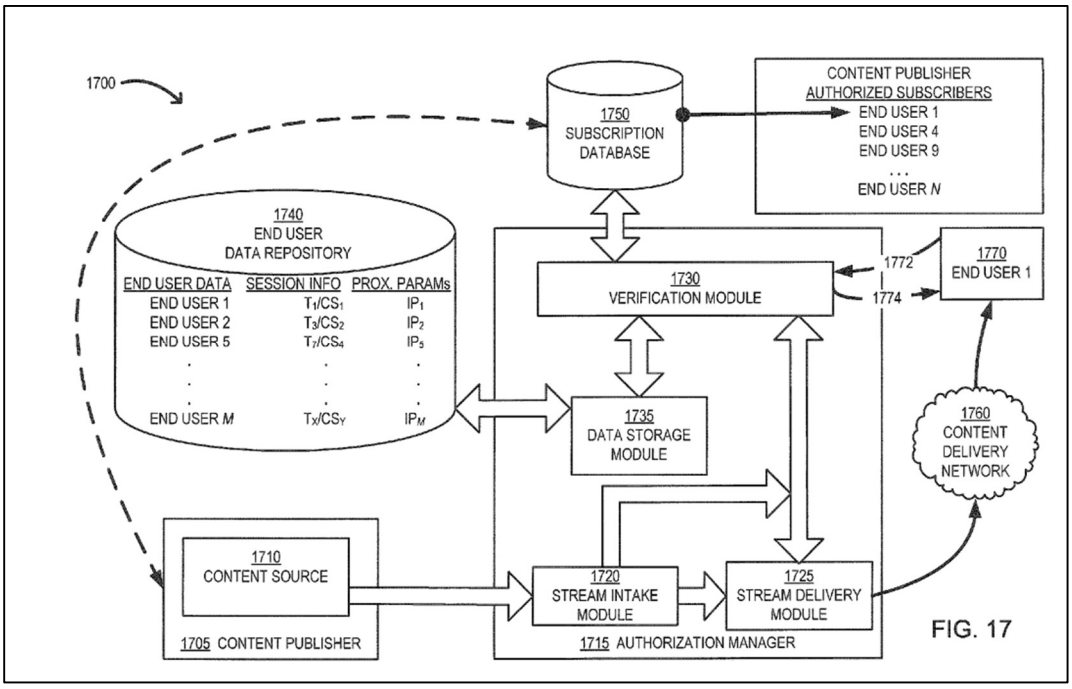


FIG. 17

'778 patent, Fig. 17.

According to the '778 patent, an end user requests certain content for viewing. '778 patent, 9:7-31, 23:36-37. In response, the system verifies ("authenticates") whether the end user is a subscriber with the appropriate permissions to view such content. *Id.*, 23:12-23. For example, the system can verify the user by checking a subscription database, which holds information related to any number of content publishers, and associates the end users with authorization ("subscriptions") to the content publisher to authenticate the user. *E.g.*, '778 patent, 29:5-12.

The '778 patent teaches other well-known means of capturing additional information to limit an end user's access to content. For example, the '778 patent teaches capturing certain "proximity parameters," which is just the patent's term for

capturing relevant geographical information such as country, region, and/or user-specific location information (i.e., IP-address) to determine whether to provide access to certain content. '778 patent, 15:32-54, 19:28-41, 23:66-24:5.

The '778 patent's recited forms of content "authentication" and verification were all known and used together in the art long before the effective date of the '778 patent. *See* Sections III.A, VI; Lin, ¶¶45-46.

IV. Level of Ordinary Skill

A person of ordinary skill in the art ("POSITA") at the time of the alleged invention of the '778 patent would have had at least a bachelor's degree in computer science, electrical engineering, or a related field, and at least two years of work/research experience in the field of content delivery management or networks. Additional educational background beyond a bachelor's degree can make up for a lack of work and/or research experience, and more than two years of relevant work and/or research experience can compensate for a lesser level of education. Lin, ¶¶47-49.

V. Claim Construction

The Board construes claims under *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b) (2018). Under this standard, terms receive their plain and ordinary meaning as understood by one of ordinary skill in the art, consistent with the disclosure and prosecution history. *Id.* Claims should only

be construed to the extent necessary to resolve a controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). No claim terms need to be construed by the Board at this time, and all should be given their ordinary meanings.

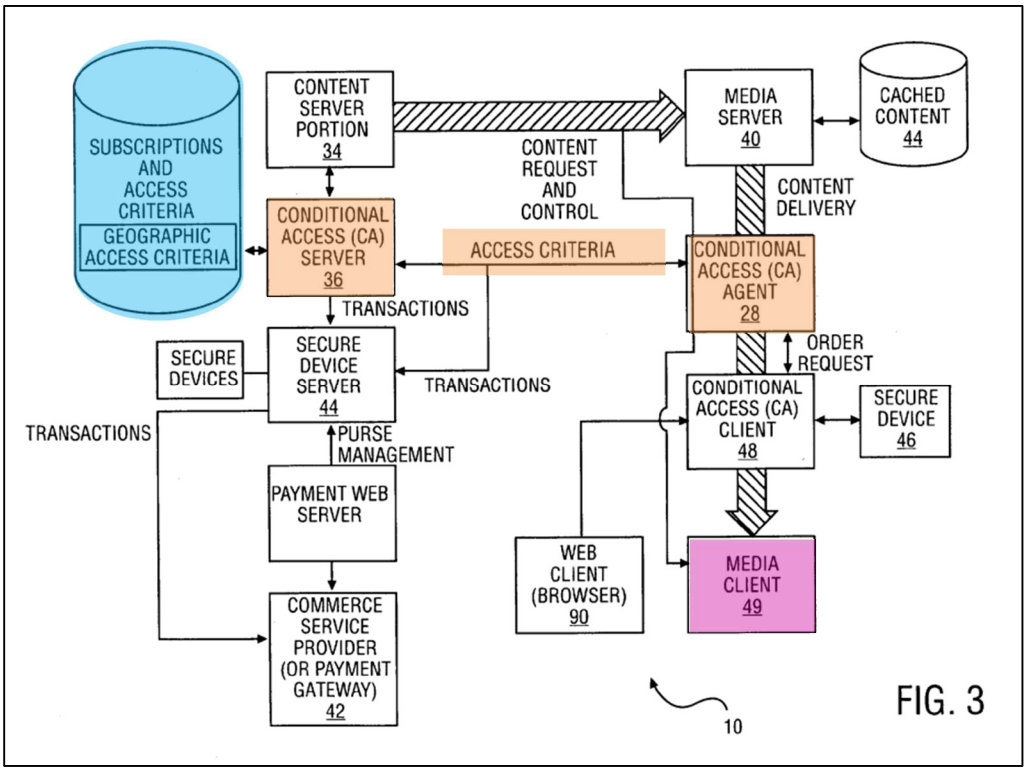
VI. Claims 1-20 Are Unpatentable Over the Prior Art

The '778 claims recite a combination of well-known prior art elements that perform their known functions to produce predictable results. Lin, ¶62. Therefore, claims 1-20 are unpatentable under 35 U.S.C. §§ 102 and 103.

A. Claims 1, 4-12, 14-20 Are Anticipated (Ground 1A) or Rendered Obvious by Fransdonk (Ground 1B)

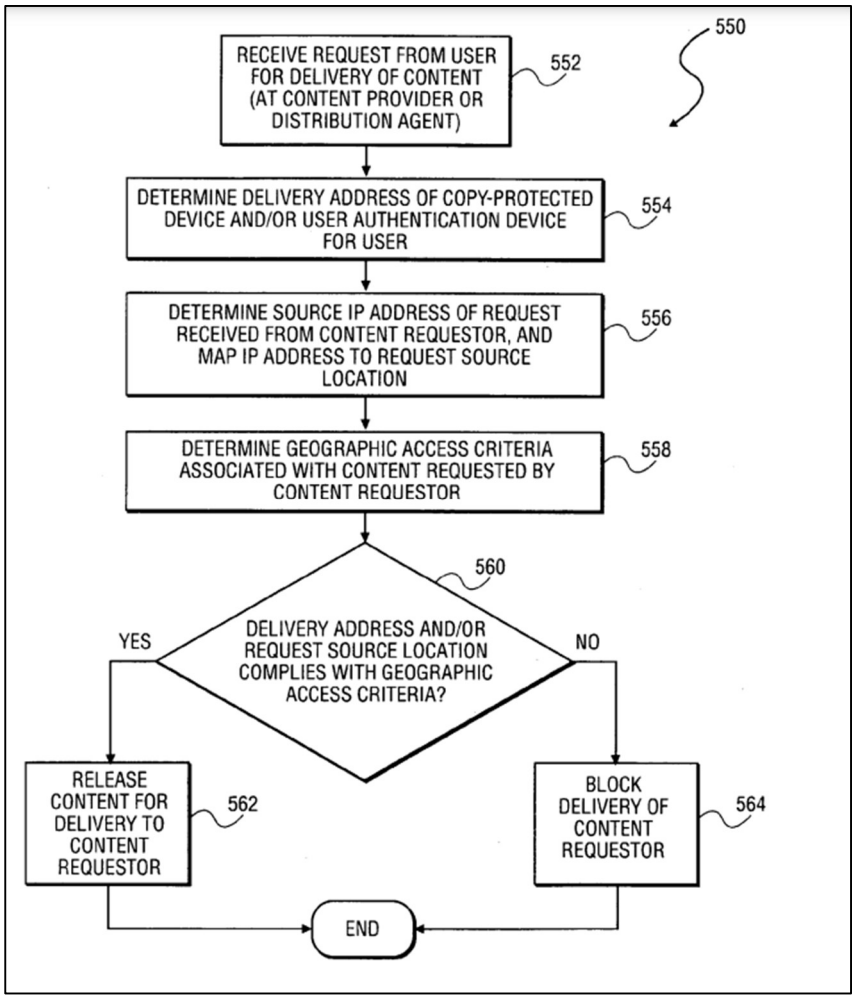
1. Fransdonk

Like the '778 patent, Fransdonk discloses methods and systems that authorize delivery of content over a network based on whether access criteria are met, like whether the geographic location complies with the geographic access criteria relative to the content requester. Fransdonk, Abstract; Lin, ¶51. The system handles requests for certain media content, verifies a content requester's **access criteria through conditional access (CA) agent 28 and conditional access (CA) server 36**, and determines whether to provide such content to the content requester based on the verification. Fransdonk, ¶¶[0060], [0062], [0092]-[0099], Fig. 3.



Fransdonk, Fig. 3 (annotated).

Fransdonk discloses providing conditional access authorization by **verifying certain subscription or other access criteria**, such as a source IP address or geographic access criteria associated with the content requester. Fransdonk, Fig. 24, ¶[0374].



Fransdonk, Fig. 24.

If the geographic information matches what the conditional access server 36 and conditional access agent 28 provide, then Fransdonk's system delivers such media content to the content requester. Fransdonk, ¶¶[0371]-[0376], Fig. 24. Otherwise, it blocks access to the media content. *See id.* Fransdonk also describes an exemplary error that blocks access to the media content, such as lacking a subscription to the content, and provides a URL for the content requester to subscribe to the content. Fransdonk, ¶[0194].

Fransdonk is analogous to the '778 patent because they are in the same field of endeavor: authenticating access requests to digital content. *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004); *compare* Fransdonk, Abstract ("A method and system…to distribute content via a network in a geographically controlled manner[.]") *with* '778 patent, Abstract ("Embodiments generally disclosed herein include computer-implemented methods for delivery of video content across a network…."); Lin, ¶54.

Moreover, because Ground 1B is a single-reference obviousness ground, it does not require showing a motivation to combine or reasonable expectation of success. *See Unification Techs. LLC v. Micron Tech. Inc.*, No. 23-1348, 2024 WL 3738401, at *6 (Fed. Cir. Aug. 9, 2024) (affirming unpatentability finding based on a single-reference obviousness that relied on expert testimony to explain how one skilled in the art would have understood the reference's disclosure and holding that "the Board was 'not required to make any finding regarding a motivation to modify' the reference.") (quoting *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1372-73 (Fed. Cir. 2019)); Lin, ¶63.

2. Independent Claim 1

a. [1.pre]: "A computer-implemented method for authorizing delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the method comprising:"

To the extent the preamble is limiting, Fransdonk discloses [1.pre] because Fransdonk discloses a computing system with machine-readable instructions to execute methods for authorizing and delivering content from a content provider as a stream to an end user. Lin, ¶64; Fransdonk, ¶¶[0022], [0051], [0404]-[0406].

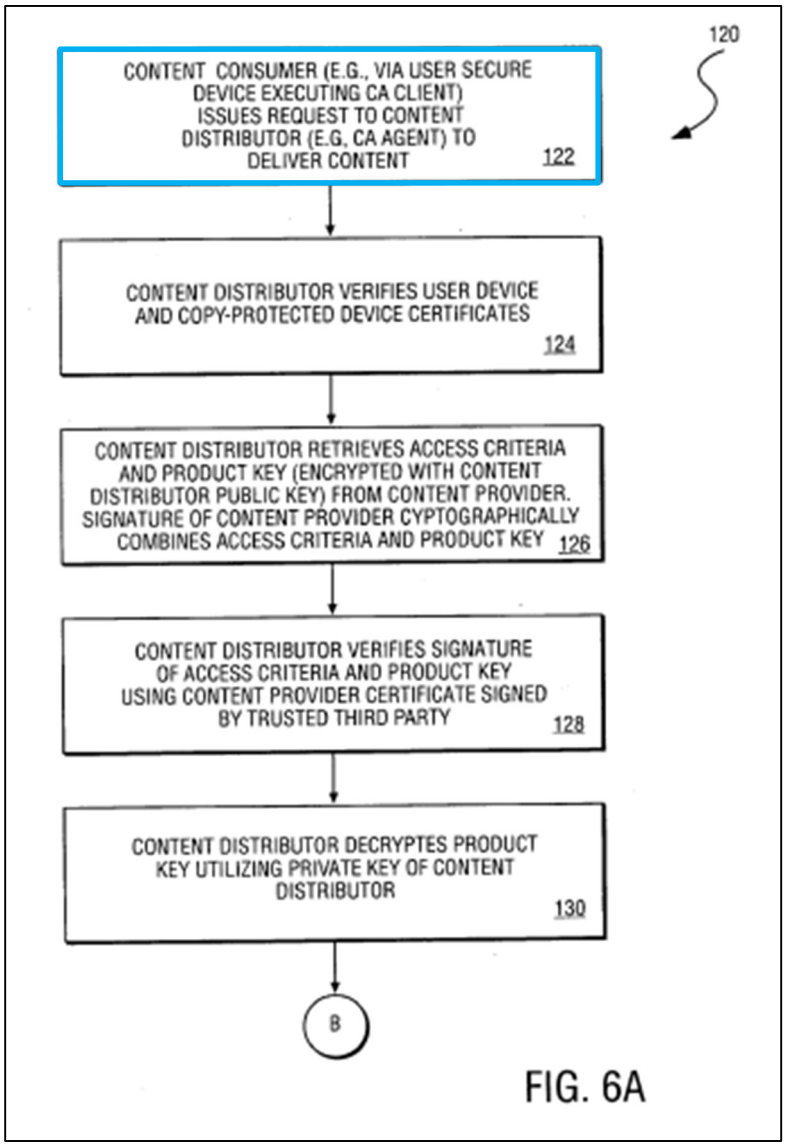
Fransdonk discloses "distribut[ing] content via a network in a geographically controlled manner…." Fransdonk, Abstract. Lin, ¶65. Fransdonk recognizes the rapid growth of the Internet made it "an exciting place to stream audio and video directly to millions of users worldwide," and addresses the ability for networks to support streaming services over a network. *See, e.g.*, Fransdonk, ¶¶[0009], [0013]. Fransdonk's solution incorporates a system architecture that supports streaming services. Fransdonk, ¶[0061] ("The conditional access agent 28 utilizes…technology ***to stream content to a viewing device***."); *see also* Fransdonk, ¶¶[0056], [0058], [0060]. Fransdonk's content also clearly includes video streaming because it uses watermarking to "embed arbitrary data into an audio or video signal." Fransdonk, ¶[0237]. Fransdonk's video stream comes from a content provider (content publisher) that is given access control "provid[ing] content providers 16 with secure geographic distribution control." Fransdonk, ¶[0369]; *see also id.*,

¶¶[0058]-[0062], [0370]. Fransdonk's method therefore includes delivery of a video stream that is associated with a content publisher. Lin, ¶65. Accordingly, Fransdonk discloses a computer-executed method for "authorizing delivery of a video stream" where the video stream is associated with the content publisher, as claimed. Lin, ¶65.

b. [1.a]: "receiving a request from the end user for delivery of the video stream to the end user across a network;"

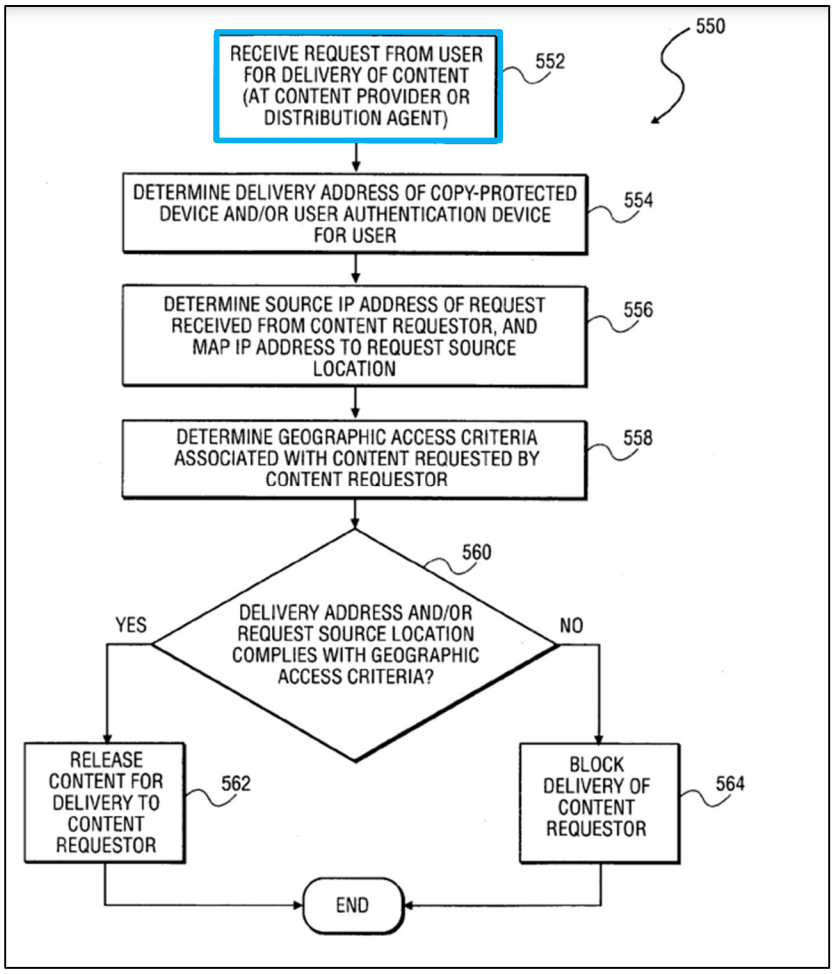
Fransdonk discloses or suggests [1.a] because it states that "[a] request is received from a content requester [(end user)] for delivery of content [(video stream)] to the content requestor via the network." Fransdonk, ¶[0022]; Lin, ¶¶66-70.

Fransdonk further discloses receiving a content request, with reference to Fig. 6A, stating that "at block 122, a content consumer [(end user)] … issues a request via the network 18 to a content distributor 20, operating a conditional access agent 28, to deliver (e.g., via streaming) particular content." Fransdonk, ¶[0217]; *see also id.*, ¶[0216].



Fransdonk, Fig. 6A (annotated).

Moreover, with reference to Fig. 24, Fransdonk discloses receiving a request from a content requester (end user) at block 552 "located at a content destination 22 for delivery of content via a network to the content destination 22." Fransdonk, ¶[0371]. With reference to Fig. 24, Fransdonk explains that the "request may be … received at conditional access agent 28." *Id.*



Fransdonk, Fig. 24 (annotated).

These requests are for delivery of the video stream "via a network to the content destination." Fransdonk, Abstract, ¶¶[0022], [0371]. For example, with reference to Figs. 2 and 3 (below), Fransdonk discloses the video stream being delivered "via a network."

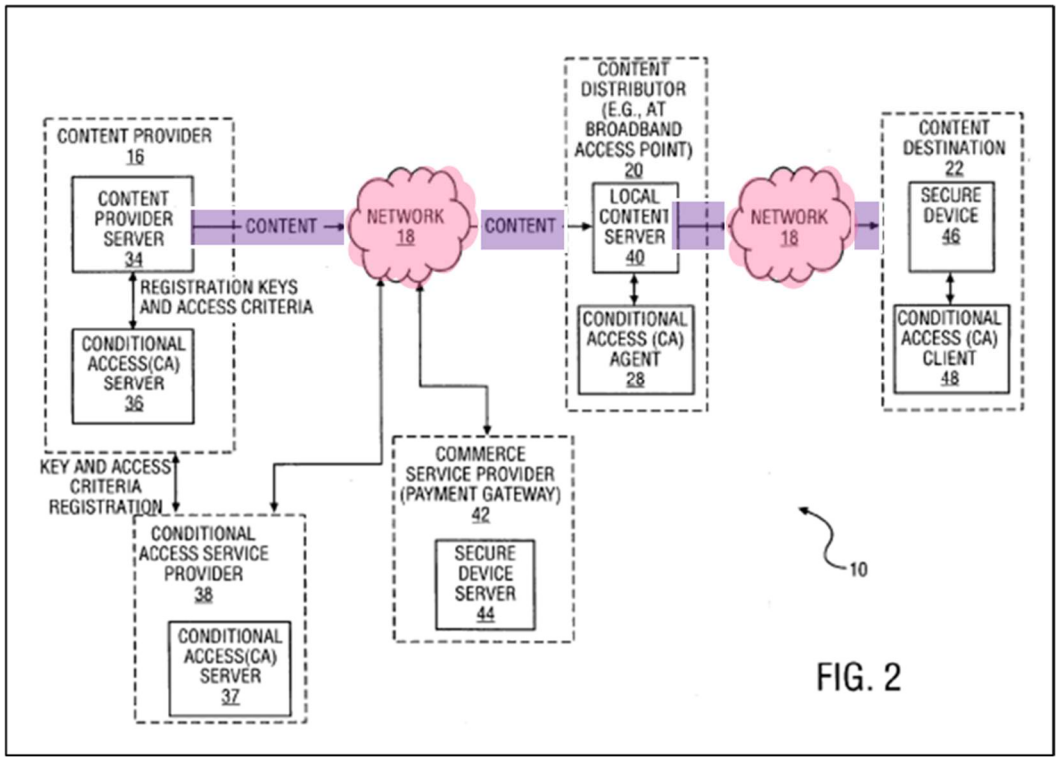


FIG. 2

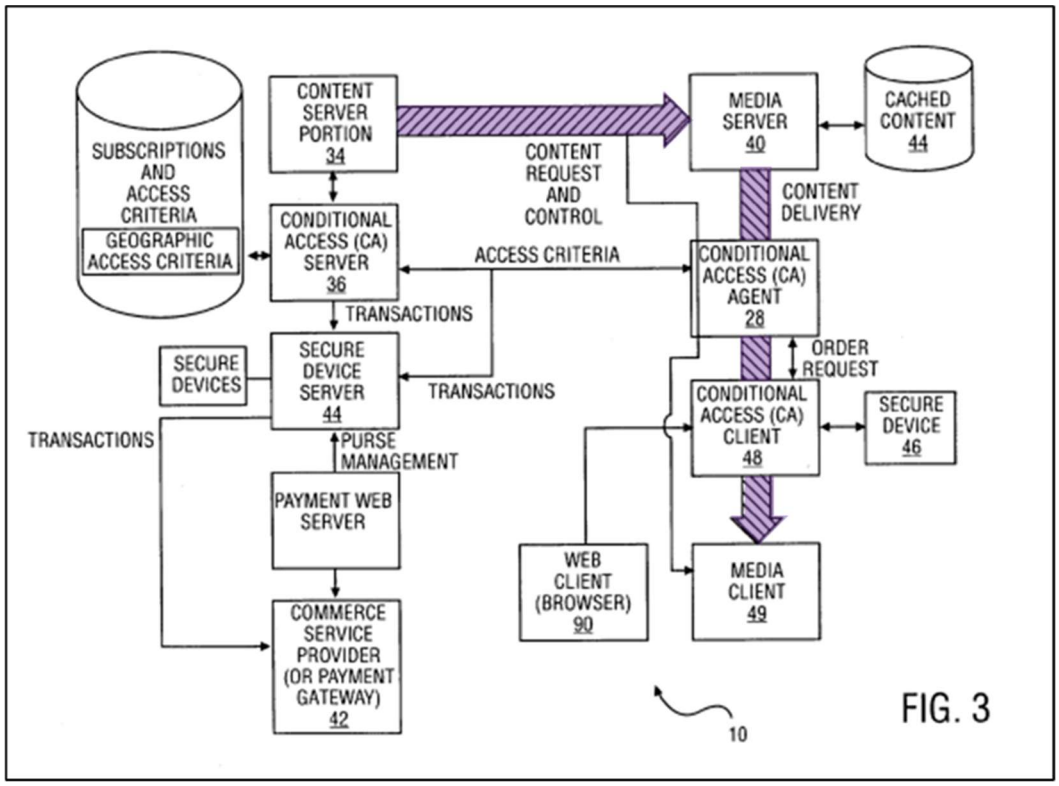


FIG. 3

Fransdonk, Figs. 2 and 3 (annotated).

Accordingly, Fransdonk discloses "receiving a request from the end user for delivery of the video stream to the end user across a network." Lin, ¶¶69-70.

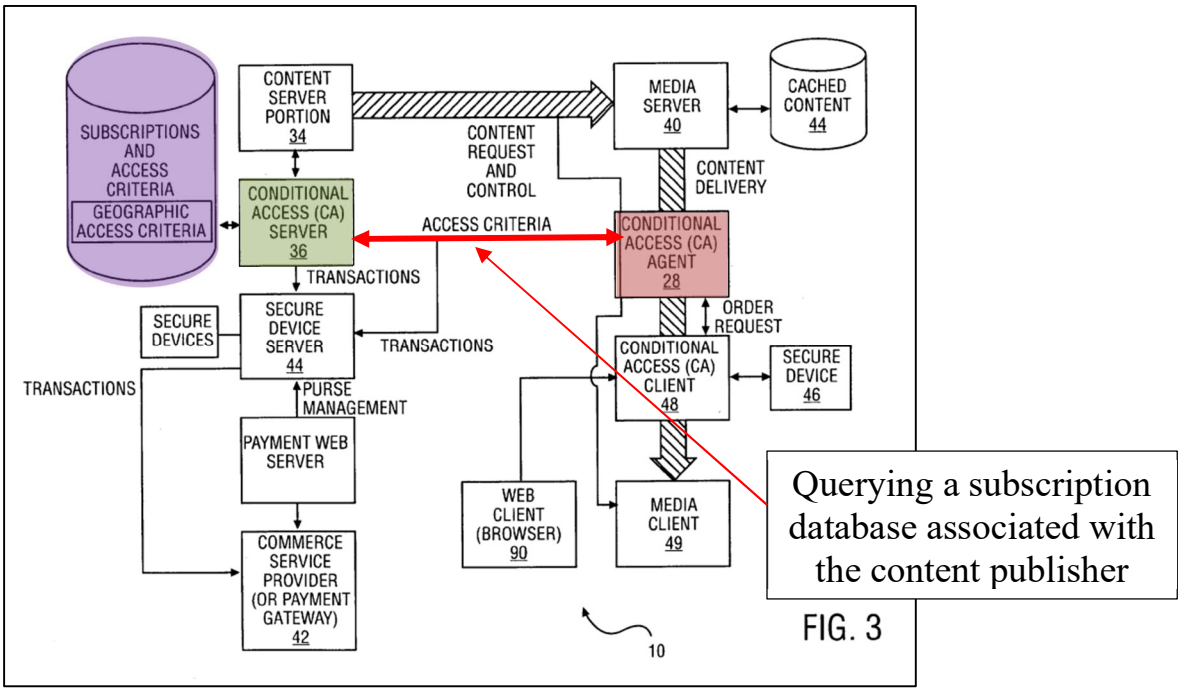
c. [1.b]: "querying a subscription database associated with the content publisher;"

Fransdonk discloses or suggests [1.b] because it discloses a **conditional access agent** that retrieves from a **conditional access server managed by a content provider** (content publisher) access criteria (subscription information) to determine, based on **database** content, whether an end user's **request for content satisfies certain criteria** (querying a subscription database). Lin, ¶¶71-77.

Fransdonk's content distribution system is "implemented by a distributed collection of **conditional access servers 36**, **conditional access agents 28**, and conditional access clients 48 that operate in conjunction with media servers … while facilitating the widespread distribution of content." Fransdonk, ¶[0062]. **Conditional access server 36** "manages subscriptions and provides monitoring and statistics tools to a content provider 16." Fransdonk, ¶[0062]. **Conditional access agent 28** "validate[s] subscriber content requests against, for example, content access criteria, local date and time, and subscriber credentials." Fransdonk, ¶[0062].

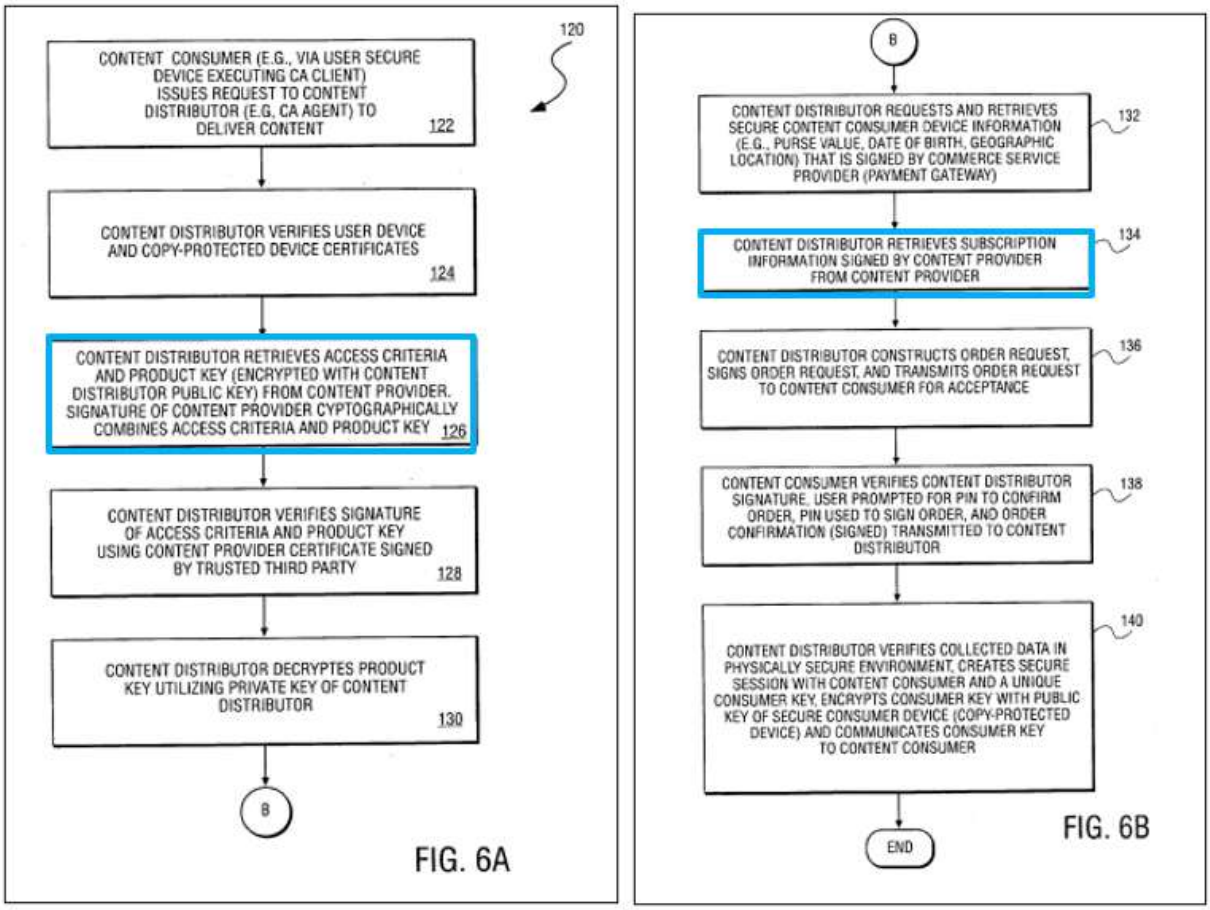
Fransdonk discloses "querying a subscription database" because its "**conditional access agent 28** retrieves the appropriate access criteria when subscribers request access to the associated content" from "**conditional access**

server 36" residing at the content provider (content publisher). Fransdonk, ¶¶[0092]-[0098]; *see also* Fransdonk, ¶[0078]. Fransdonk's **conditional access server 36** includes a number of databases (Fransdonk, ¶[0028]) that store access criteria including subscription information because **conditional access server 36** "allows content providers 16 to create and manage **content products** (subscription types)" and "**[m]anagement of subscriptions** (generation, storage and distribution)…." Fransdonk, ¶¶[0091]-[0096]; *see also* Fransdonk, ¶[0069] ("(4) Pay-per-view, pay-per-time and ***subscription based access***."), ¶[0078]. Indeed, the user information is stored in such a way at the conditional access server 36 that Fransdonk teaches retrieval (querying) can be performed efficiently by conditional access agent 28. Fransdonk, ¶[0098]. Fransdonk's subscription database being queried by the conditional access agent via the conditional access server is shown in Fig. 3.



Fransdonk, Fig. 3 (annotated).

Fransdonk's conditional access agent 28 also queries the conditional access server and subscription database because, as shown in Fig. 6A at block 126, "conditional access agent 28[] retrieves access criteria and a product key related to the requested content." Fransdonk, ¶[0226]. Later in the flow diagram of Fig. 6B, at block 134, Fransdonk's "conditional access agent 28 … receives the subscription information from the conditional access server 36." Fransdonk, ¶[0226].

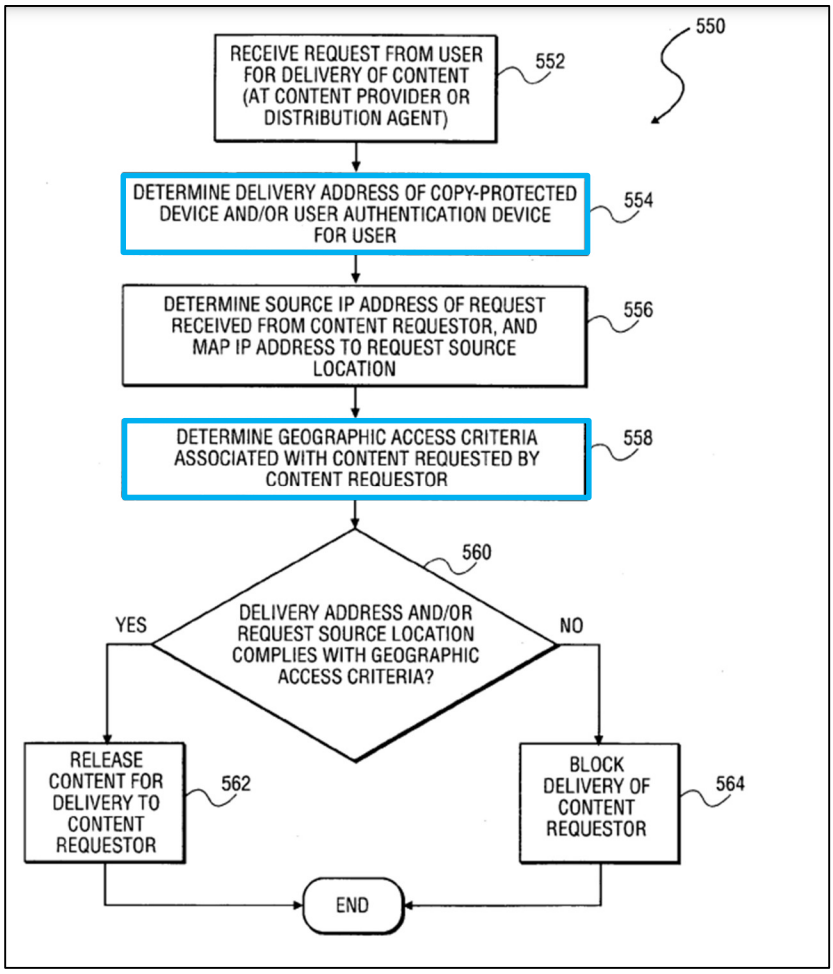


Fransdonk, Figs. 6A and 6B (annotated).

While Fransdonk teaches access criteria including subscriptions generally, one type of access criteria/subscription data retrieved from Fransdonk's subscription database associated with conditional access server 36, based on the query, is geographic access criteria, as shown in Figure 3 above. A POSITA would have understood geographical access criteria to be a form of subscription data because, as the '778 patent explains, it "relate[s] to various end users authorized to receive content from [a] content publisher" including "information related to traditional

satellite and/or cable television services provided by [the] content publisher." '778 patent, 22:16-29; Bacso, ¶¶[0084], [0086]-[0087]; Lin, ¶75. Dependent claim 7 confirms this understanding because it defines subscription criteria as including geographic criteria. *Id.*, claim 7. As Fransdonk explains, its geographical access criteria, stored alongside other subscription data, is used to confirm that a particular user is authorized to receive content from a particular content publisher via a particular service. Fransdonk, Abstract, ¶¶[0372], [0375]-[0376], Fig. 24.

Fransdonk discloses querying the conditional access server 36 for geographic subscription information, as shown in Fig. 24. "At block 554, the conditional access agent 28, in the manner described above, retrieves access criteria associated with the request[ed] content from an appropriate conditional access server 36 operated via a content provider 16," which "includes geographic access criteria specifying geographic regions (e.g., countries, states, provinces, counties, towns, municipal areas, etc.) and access conditions associated with those geographic regions." Fransdonk, ¶[0372]. And "[a]t block 558, the conditional access agent 28 examines the geographic access criteria, included in the access criteria retrieved from the conditional access server." Fransdonk, ¶[0375].



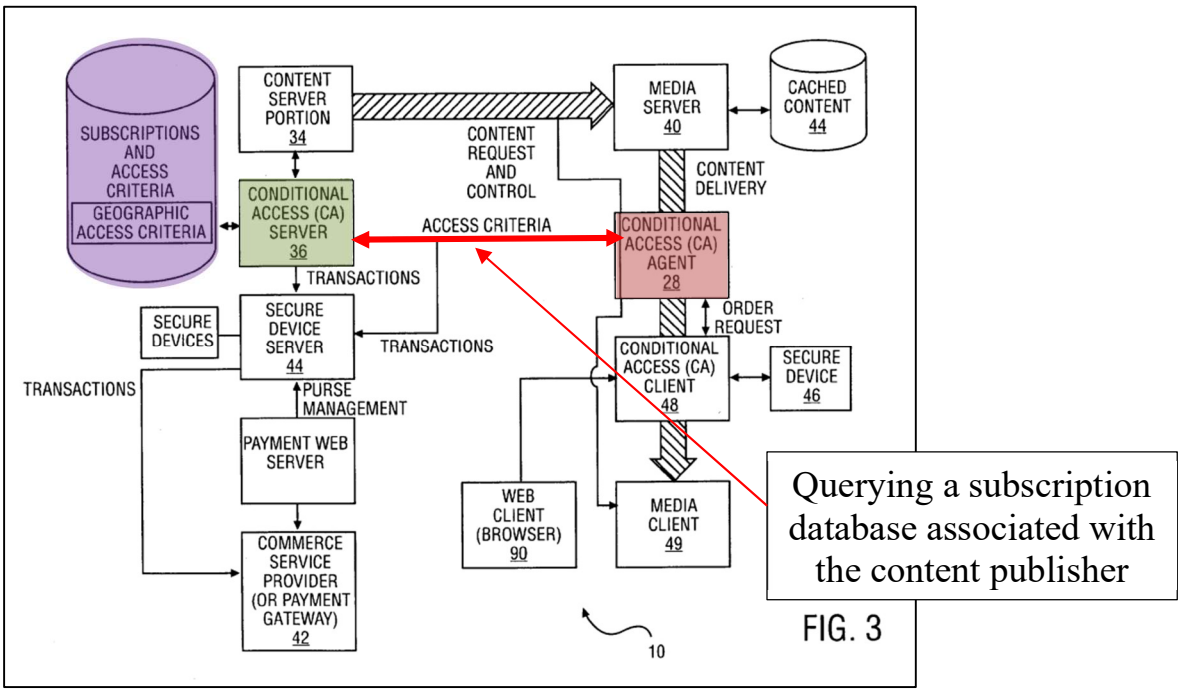
Fransdonk, Fig. 24 (annotated).

Accordingly, Fransdonk's method discloses "querying a subscription database associated with the content publisher" in the form of access criteria comprising one or both of subscription information and geographic criteria. Lin, ¶¶76-77.

d. [1.c]: "in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream; and"

Fransdonk discloses or suggests [1.c] because its conditional access agent 28 receives the access criteria (reply from the subscription database) from the conditional access server and subscription database and determines whether the content requester (end user) can receive the requested content based on the required criteria (has authorization to receive delivery of the video stream). Lin, ¶78.

As explained for limitation [1.b], Fransdonk's conditional access agent 28 queries conditional access server 36 and associated subscription database. Lin, ¶79.

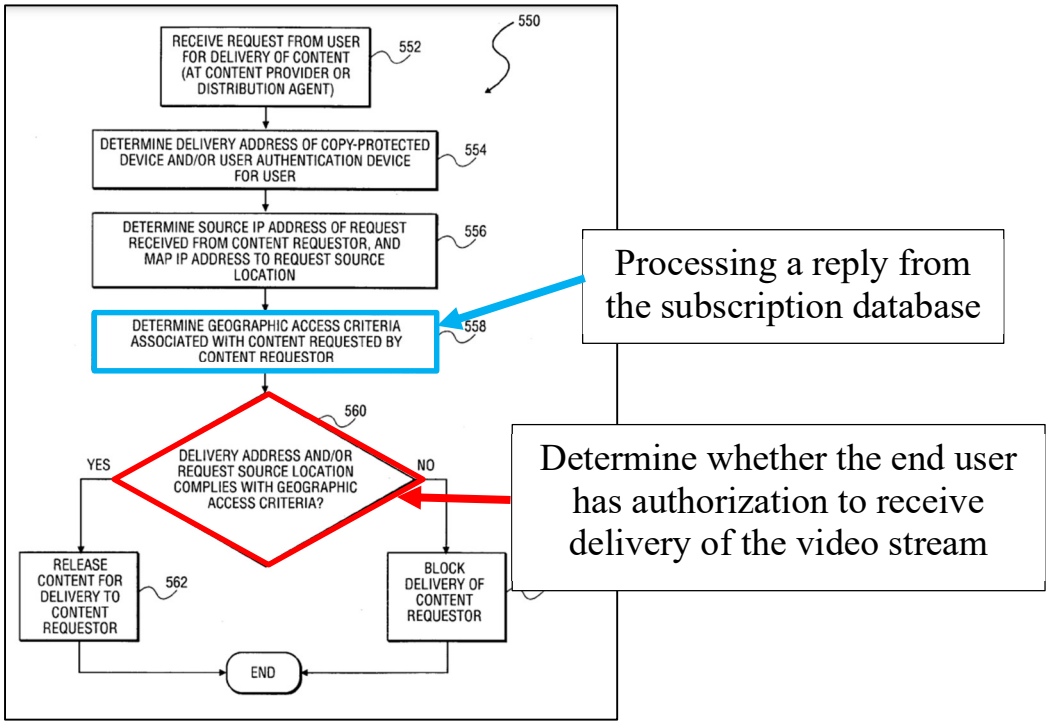


Fransdonk, Fig. 3 (annotated).

Based on the information Fransdonk's conditional access agent 28 retrieves from the conditional access server 36 and subscription database, Fransdonk determines whether the user is authorized to receive delivery of the requested video stream content. Fransdonk states that its "conditional access agent 28 is a cryptographic component that insures [sic] that access criteria, as defined by content provider 16 are enforced." Fransdonk, ¶[0062]; *see also* Fransdonk, ¶[0079] ("conditional access agents 28 … act as 'brokers' enforcing the security settings that are associated with content by content providers 16"). To ensure access criteria is enforced, conditional access agent 28 performs "a verification function that includes verification of content destination (e.g., subscriber) requests for secure content against access criteria defined by a content provider 16." Fransdonk, ¶[0136].

For geographic access criteria, Fransdonk additionally describes that the authorization process performed by the conditional access agent 28 includes determining both geographic access criteria associated with the content and whether the geographic location complies with such access criteria. Fransdonk, ¶¶[0372]-[0376]. Fransdonk explains, with reference to Fig. 24, that at "block 554, the conditional access agent 28 … retrieves access criteria" including "geographic access criteria." Fransdonk, ¶[0372]. And, also at block 554, "the conditional access agent 28 also commences a content requestor or authentication process" to determine the delivery location of the user. Fransdonk, ¶[0373]. "At block 558, the conditional

access agent 28 examines the geographic access criteria, included in the access criteria retrieved from the conditional access server 36" (Fransdonk, ¶[0375]), and at "decision block 560, the conditional access agent 28 makes a determination as to whether the delivery address … compl[ies] with the geographic access criteria" (Fransdonk, ¶[0376]). *See also* Fransdonk, ¶[0022].



Fransdonk, Fig. 24 (annotated).

Fransdonk, therefore teaches "in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream." Lin, ¶¶80-81.

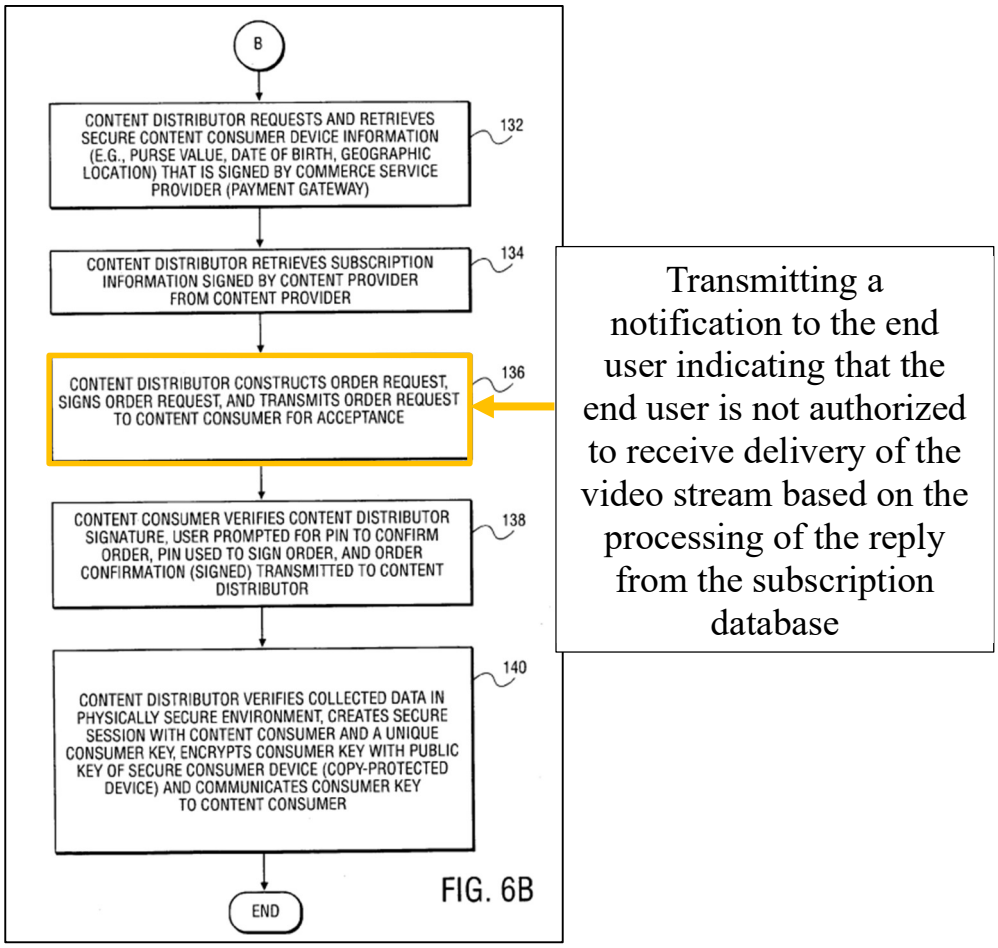
e. [1.d]: "performing at least one of: transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream."

When presented with mutually exclusive steps of a claim, Petitioner need only demonstrate one such limitation is disclosed to anticipate the limitation. *See Apple, Inc. v. Evolved Wireless LLC*, IPR2016-01177, Paper 27 at 13 (PTAB Dec. 20, 2017) ("[S]ince there can be only one value for each of A and B at a given time, … as used here must mean 'considering A, B, or both.'"). Fransdonk, however, teaches both limitations. Lin, ¶82.

i. [1.d.i]: "transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and"

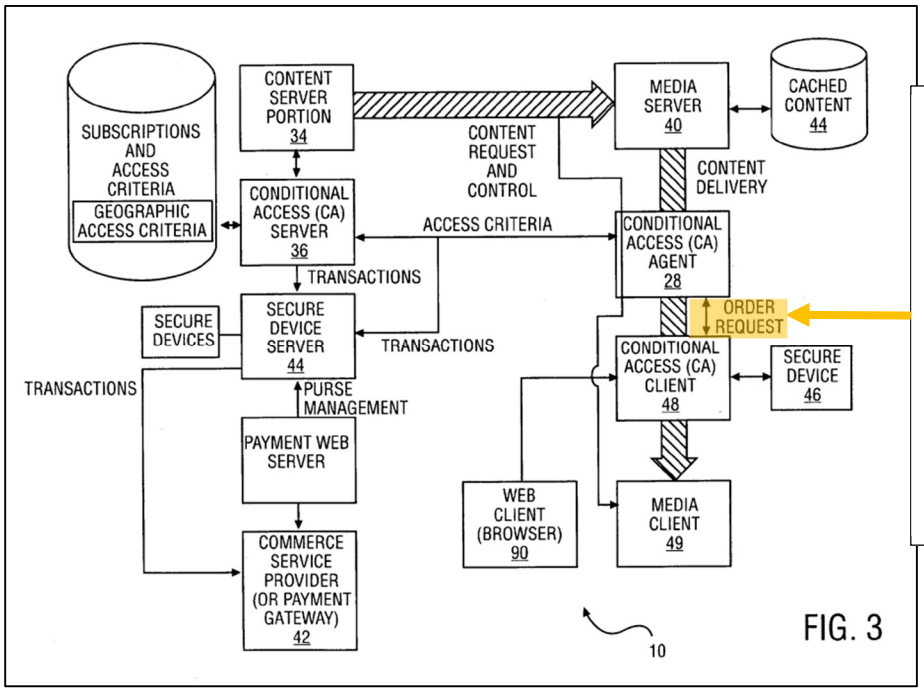
Fransdonk discloses or suggests [1.d.i] for multiple reasons. As explained for limitation [1.c], Fransdonk discloses "processing of the reply from the subscription database" to determine whether the user is authorized to receive delivery of the video stream. If the user is not authorized to receive the video stream based on the access criteria, Fransdonk teaches transmitting three potential notifications to the end user.

First, Fransdonk teaches the claimed notification under Sandpiper's apparent interpretation in parallel district court proceedings. Sandpiper alleged that this "notification" was satisfied by offering a subscription to the user. *See* Ex. 1012 at 6 ("Free preview has ended . . . start a free trial"); *id.* ("Sign up to watch"); *id.* at 7 ("Add to membership"). Similar to Sandpiper's contentions, Fransdonk discloses that if a user does not have a current subscription to receive content ("the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database"), then Fransdonk teaches allowing a user to purchase such subscription by transmitting an order request to the consumer ("transmitting a notification to the end user.") Fransdonk, ¶[0227]. Fransdonk explains, with reference to Fig. 6B, that if a user does not have a current subscription to view requested content, "conditional access agent 28 of content distributor 20 constructs an order request to a conditional access client 48 of the content consumer for acceptance" which consists "of a number of order options, if applicable (e.g., a pricing of $8.00, or $4.00 for a predetermined amount of time plus $1.00 per minute thereafter)." Fransdonk, ¶[0227].



Fransdonk, Fig. 6B (annotated).

Because the subscription order request is sent to "conditional access client 48 of the content consumer for acceptance," a POSITA would have understood that the order request is a notification to the end user because Fransdonk explains that the conditional access client 48 manages an interface to the content requester (i.e., end user). Fransdonk, ¶[0061]; Lin, ¶¶83-85.



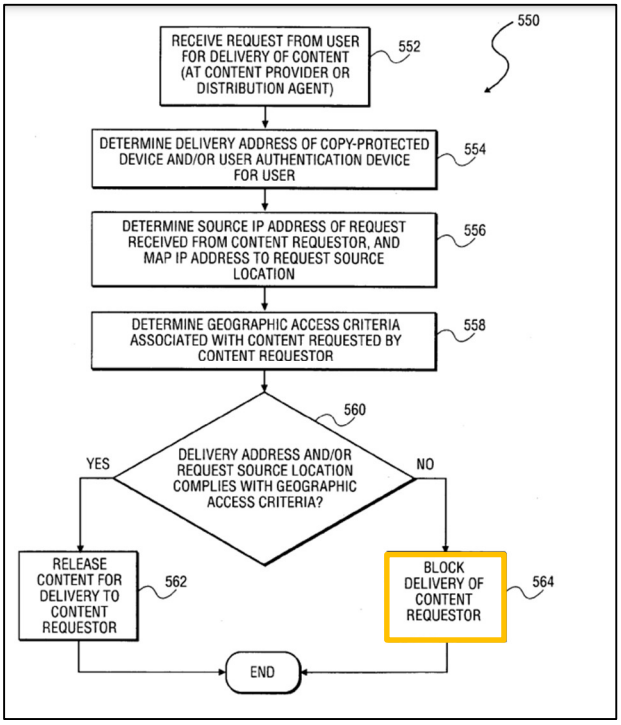
Transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database

Fransdonk, Fig. 3 (annotated).

Second, building on the first notification (subscription order request), Fransdonk also teaches sending an error message to a user if a subscription request is not successfully completed. Fransdonk, ¶[0194]. Fransdonk explains, "[i]f a subscription request is not successfully completed, the [conditional access] client 48 displays an error message to the user" including both "an error code and an English-language error description." Fransdonk, ¶[0194]. The error notification also may identify "a site for which appropriate subscription may be obtained if the lack of such a subscription results in the error message." Fransdonk, ¶[0194].

Third, for geographical access criteria, Fransdonk expressly discloses that, if "the end user is not authorized to receive delivery of the video stream" the system

blocks access to the content, wherein the user does not receive the requested content. Fransdonk, ¶[0376].



Fransdonk, Fig. 24 (annotated).

A POSITA would have been motivated to send an error message to the end user in such circumstances, as taught by Fransdonk for lack of subscription, because such error notifications were well-known in the art, Fransdonk already discloses the means for transmitting and displaying such an error notification, and a skilled artisan would have recognized the benefits of advising a consumer of the reasons requested content could not be delivered. Lin, ¶88. As Dr. Lin explains, it was well known to provide notifications to end users over a streaming network when a request for content failed. Bi, ¶[0167]; Lin, ¶88. Implementing Fransdonk's error messaging

means into a notification function to an end user would provide improved commercialization of the digital content. For example, a POSITA would have found it straightforward to implement a notification to an end user based on the processing of a content database query. Bi, Figs. 48-50, ¶¶[0189]-[0190]; Lin, ¶88. Fransdonk teaching to provide the error message with a URL link to the unauthorized end user itself is a motivation that gives added flexibility to the content delivery system, adding monetization efforts that contribute to the stated goal of the '778 patent. Lin, ¶¶84-88; '778 patent, 1:36-44; Fransdonk, ¶[0194].

ii. [1.d.ii]: "initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream."

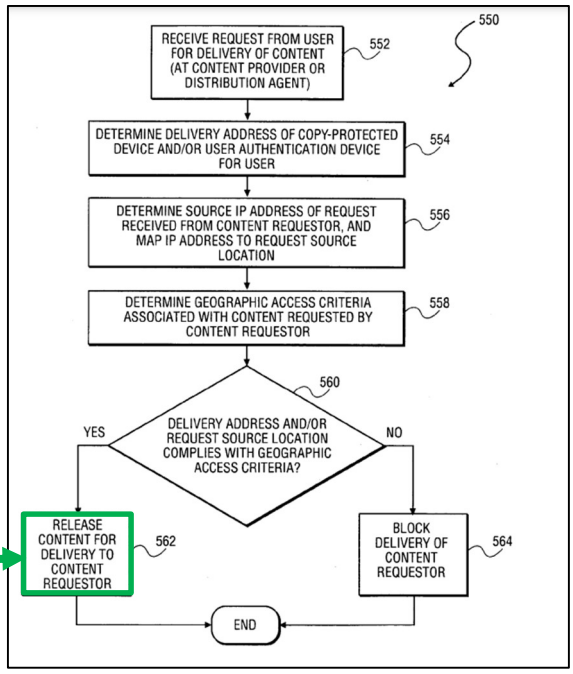
Fransdonk discloses or suggests [1.d.ii] because if the conditional access agent determines the content requester (end user) meets the access criteria (based on the processing of the reply from the subscription database), Fransdonk initiates delivery of the video stream to the end user. Lin, ¶¶89-91.

First, as explained for [1.c], Fransdonk generally explains that conditional access agent 28 "validate[s] subscriber content requests against, for example, content access criteria, local date and time, and subscriber credentials." Fransdonk, ¶[0062]. Conditional access agent 28 operates to "authenticate a content destination 22" (i.e.,

where the content request originates) by evaluating the content request ***based on*** the access criteria specified by the content provider 16. Fransdonk, ¶[0060]. Fransdonk's credentialing between the conditional access agent 28 and conditional access server 36 allow content providers to create access criteria for review and processing. Fransdonk, ¶¶[0103]-[0104]. To wit, conditional access agent 28 "interfaces with the conditional access server 36 to query subscriptions," and acts as a "broker" to then send the requested content to the correct content destination ***based on*** the response from the subscription query. Fransdonk, ¶¶[0079], [0136], [0146]. Assuming the correct credentials are met, Fransdonk teaches forwarding the media content ("initiating delivery of the video stream") as indicated by its connection to media client 49 that uses the "Real Time Streaming Protocol." Fransdonk, ¶[0149].

Second, for geographic access criteria, Fransdonk discloses "initiating delivery of the video stream" because upon the geographic access criteria against the delivery location, the conditional access agent 28 **will release the content to the content requester (end user)**. Fransdonk explains, with reference to Fig. 24, that if "the delivery address … determined at block 554 … compl[ies] with the geographic access criteria," "at block 560, the conditional access agent 28 released the requested content … for delivery to the content destination 22 of the content requester." Fransdonk, ¶[0376]; *see also* Fransdonk, ¶[0022].

Initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream.



Fransdonk, Fig. 24 (annotated).

3. Claim 4:

Fransdonk discloses claim 4. Lin, ¶¶92-98.

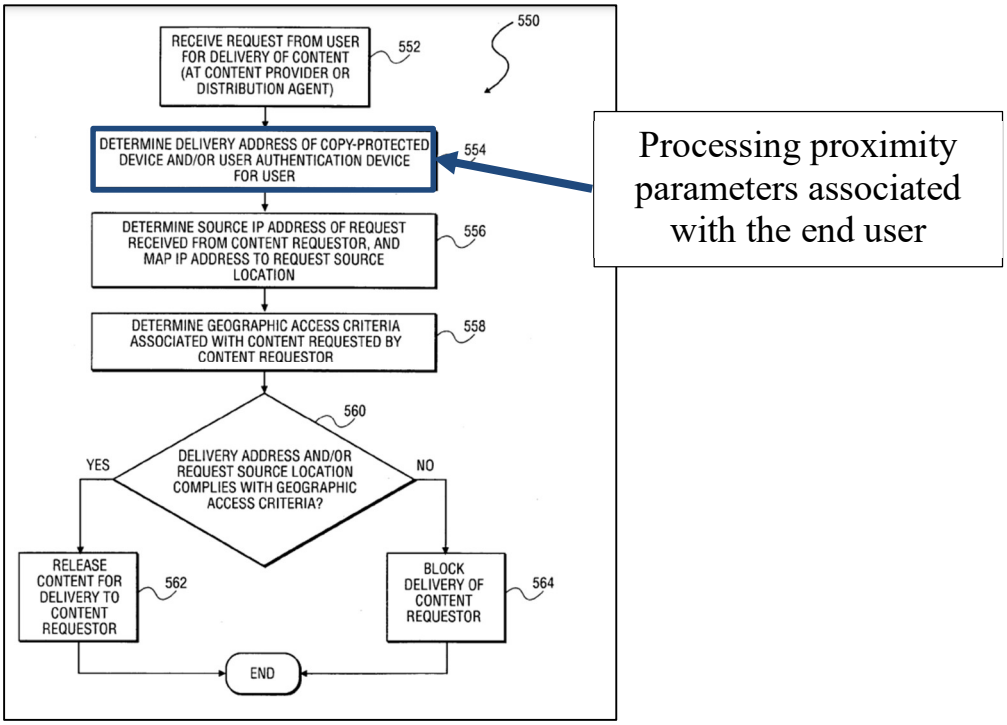
a. [4.a]: "The computer-implemented method as in claim 1, further comprising: processing proximity parameters associated with the end user, wherein the proximity parameters specify a geographic location of the end user to where video content is transmitted;"

Fransdonk discloses [4.a] because it compares geographic access criteria to a content delivery location (processing proximity parameters associated with an end user, specifying a geographic location to where video content is transmitted).

As explained for [1.c] with respect to geographic access criteria, Fransdonk's "conditional access agent 28 … commences a content requestor or authentication process" to confirm that geographic access criteria are met (processing proximity

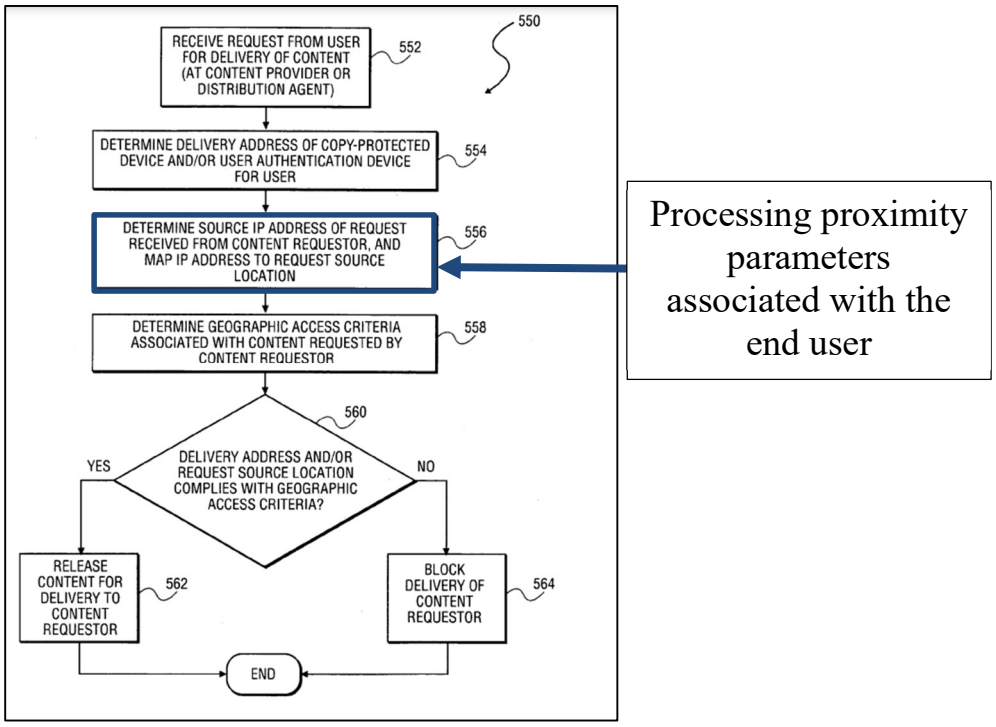
parameters). Fransdonk, ¶[0373]. Fransdonk discloses authenticating against geographic access criteria in two different ways. Lin, ¶93.

First, Fransdonk discloses "performing a lookup to determine the physical delivery address" of the user or the user's device. Fransdonk, ¶[0373].



Fransdonk, Fig. 24 (annotated).

Second, Fransdonk discloses that "the conditional access agent 28 determines the source IP address of the request received from the content requestor at the content destination 22, and attempts to map the source IP address to a geographic location." Fransdonk, ¶[0374].



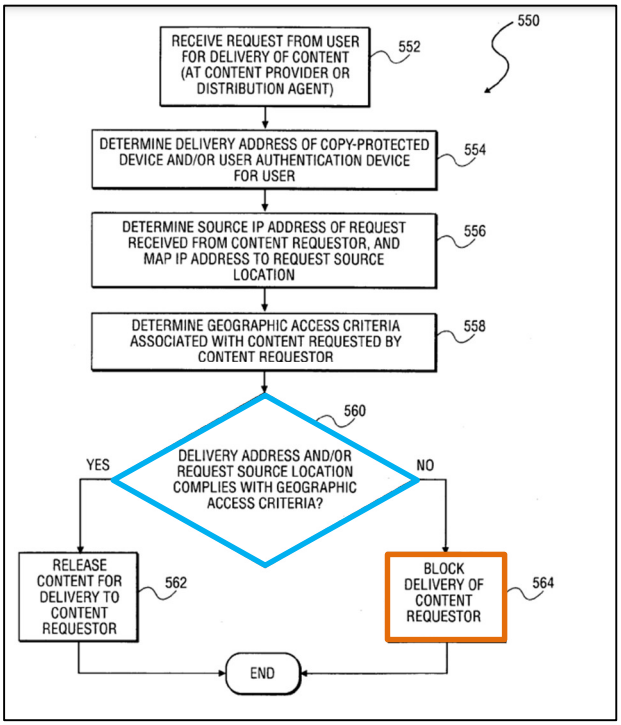
Fransdonk, Fig. 24 (annotated).

Each of the physical delivery address and the IP address satisfies the claimed "proximity parameters" because both "specify a geographic location of the end user to where video content is transmitted," as claimed. Fransdonk, ¶¶[0373]-[0374].

Moreover, each of Fransdonk's proximity parameters (both the physical delivery address and the IP address) are "processed" as claimed because, with reference to Fig. 24, Fransdonk explains that "the conditional access agent 28 makes a determination as to whether the delivery address (or addresses) determined at block 554 and/or the geographic location associated with the source IP address determined at block 556 comply with the geographic access criteria." Fransdonk, ¶[0376]. Lin, ¶97.

b. [4.b] "based on the processing of the proximity parameters, determining that the end user is not authorized to receive the video stream; and"
[4.c] "restricting delivery of the video stream to the end user."

Fransdonk discloses [4.b] and [4.c] because it discloses determining whether the address and/or IP address (i.e., proximity parameters) associated with the content requester's geographic location complies with the geographic access criteria. Fransdonk, ¶[0376]. According to Fransdonk, if there is a "negative determination," it restricts delivery of the video stream by blocking the content requester from accessing the requested content (i.e., "restricting delivery of the video stream to the end user"). Fransdonk, ¶[0376], Fig. 24 (below); *see also id.*, ¶[0377]; Lin, ¶98.



Fransdonk, Fig. 24 (annotated).

4. Claim 5: "The computer-implemented method as in claim 4, wherein determining that the end user is not authorized to receive the video stream comprises: given a relative time associated with the receipt of the request from the end user, determining whether the video stream should be blacked out for at least a time period associated with the relative time in relation to the geographic location of the end user."

Fransdonk discloses claim 5. Lin, ¶99.

Fransdonk discloses associating a relative time of the request from the end user by the content access agent 28 making real-time evaluations for content requests. *See* Fransdonk, ¶[0060] ("[A] conditional access agent 28 may evaluate a content request … based on access criteria specified by a content provider 16, ***local date and time information***, and user credentials and authentication."). Fransdonk also discloses determining whether to blackout content for a content requester in a specific geographic region given a relative time because it expressly discloses as part of its core functions providing "access control ***on the basis of region and date/time***." Fransdonk, ¶[0070]; Lin, ¶99; *see also* Fransdonk, ¶[0019] (describing desire to provide "a content distributor with a degree of geographic control over the distribution of content" for specific content, such as blocking a certain country's users from viewing a live game broadcast based on exclusive broadcasting rights). Indeed, Fransdonk teaches capturing such blackout information in its associated "ACProfileRegionBlackout" and "ACProfileCountryBlackout" tables. *See* Fransdonk, ¶¶[0128]-[0129] (tables); *see also id.*, ¶[0130] (capturing time-based and

date-based restrictions, including "if access must be blocked during certain hours" ['TimeWindowFlag'], "if access must be blocked before or after [a] certain date range" ['DateWindowFlag'] as well as the "local time to start/stop blocking access" ['TimeWindowStart','TimeWindowEnd']). Lin, ¶99.

[0128] The table ACProfileCountryBlackout represents the regions that are to be blacked out for a certain profile.

Field	Description
MerchantId	
ProfileId	
CountryId	Country to be blacked out

MerchantId, ProfileId, and CountryId form the unique key.

[0129] The table ACProfileRegionBlackout represents the regions that are to be blacked out for a certain profile.

Field	Description
MerchantId	
ProfileId	
CountryId	Country to be blacked out
RegionId	Region to be blacked out

MerchantId, ProfileId, CountryId and RegionId form the unique key.

Fransdonk, ¶¶[0128]-[0129].

5. Claim 6: "The computer-implemented method of claim 4, wherein restricting delivery of the video stream to the end user is in accordance with black out rules associated with the content publisher, the black out rules having associated time restrictions and geographic restrictions prescribed by the content publisher for the end user."

Fransdonk discloses claim 6. Lin, ¶100.

Fransdonk expressly discloses blacking out content in accordance with blackout rules with associated time and geographic restrictions as a core function of

its disclosure. Fransdonk, Abstract, ¶[0070] ("access control ***on the basis of region and date/time***."); *see also* Fransdonk, ¶¶[0128]-[0129] (capturing countries and regions that "are to be blacked out" for certain user profiles); ¶[0130] (capturing time-based and date-based restrictions including "if access must be blocked during certain hours" ['TimeWindowFlag'], "if access must be blocked before or after [a] certain date range" ['DateWindowFlag'], as well as the "local time to start/stop blocking access" ['TimeWindowStart','TimeWindowEnd']). Fransdonk likewise discloses that its blackout rules are associated with the content publisher because conditional access server 36 and conditional access agent 28 ensure that access criteria "as defined by content providers" (i.e., the content publishers) are enforced. Fransdonk, ¶[0062]; Lin, ¶101.

6. Claim 7: " The computer-implemented method of claim 4, wherein restricting delivery of the video stream to the end user is in accordance with subscription parameters of the content publisher for a group of end users, the subscription parameters including at least one of a time restriction and a geographic restriction, and wherein the end user is a member of the group of end users to which the subscription parameters apply."

Fransdonk discloses claim 7. Lin, ¶102.

As explained for claims 5 and 6, Fransdonk discloses restricting delivery based on subscription parameters that includes both time and geographic restrictions. Fransdonk, Abstract, ¶¶[0069], [0070] ("access control ***on the basis of region and***

date/time"). Fransdonk teaches content publishers can create certain "content products" that provide durations including start and end dates (i.e., time restrictions), which are associated with subscriptions. Fransdonk, ¶[0101]. The system captures access criteria under which items are to be provided to certain subscribers in its "ACProfileSet" table. Fransdonk, ¶¶[0060], [0066], [0130]. The ACProfileSet table captures information limiting groups of subscribers based on time (e.g., TimeWindowFlag, TimeWindowStart, TimeWindowEnd, DateWindowFlag, DateWindowStart, DateWindowEnd). *See* Fransdonk, ¶[0130] (below); Lin, ¶103.

Field	Description
MerchantId	
ProfileId	
CountryId	
RegionId	
SetId	Sequence number (order is of importance)
SubscriptionFlag	
ProductIssuerId	
ProductId	
PriceFlag	
PGWId	Payment gateway ID
PurchasePrice	
TimePriceFlag	
Time	Viewing time associated with purchase price
TimePrice	(Used for pricing such as 1$ per minute)
ViewTime	Viewing time associated with recurring price (e.g. 1 minute in case of 1$ per minute)
LoyaltyFlag	True if subscriber can earn loyalty points.
LoyaltySchemeId	Loyalty scheme such as air-miles or FFP (future use)
LoyaltyPoints	Number of points (future use)
ParentalFlag	True if access is restricted to certain minimal age
ParentalCode	Minimum age
TimeWindowFlag	True if access must be blocked during certain hours
TimeWindowStart	Local time to start blocking access
TimeWindowEnd	Local time to stop blocking access
DateWindowFlag	True if access must be blocked before or after certain date range
DateWindowStart	
DateWindowEnd	
FormattedAC	Formatted access criteria (future use for improved performance)

MerchantId, ProfileId, CountryId, RegionId and SetId form the unique key.

Fransdonk, ¶[0130] (ACProfileSet Table) (annotated).

Fransdonk discloses or suggests applying a certain subscription parameter to a group of end users because a content publisher has the functionality to limit entire groups of subscriptions based on, *inter alia*, time restrictions. *See* Fransdonk, ¶¶[0101], [0130]. Lin, ¶104.

7. Claim 8: "The computer-implemented method as in claim 4, wherein restricting delivery of the video stream comprises: terminating the delivery of the video stream to the end user if delivery of the video stream to the end user has already been initiated."

Fransdonk suggests claim 8. Lin, ¶105.

Fransdonk discloses sending requested media content to content destinations 22 that involves streaming media via satellite multicast or live broadcast. Fransdonk, ¶¶[0054], [0056], [0081]. The streamed media is then displayed at traditional end user media terminals such as personal computers or set-top boxes. *Id.* If conditional access agent 28 authenticates a content request, it will stream content to a destination viewing device. Fransdonk, ¶[0061]. Prior to verifying the content request, a content publisher establishes access criteria, which Fransdonk allows certain time windows to be blacked out. *See* Fransdonk, ¶[0130]; *see also supra* claims 5-7. Because Fransdonk handles live broadcasts across channels, a POSITA would have understood that certain programs may be broadcast in such a way where a channel has no blackout/restrictions for a given program, while subsequent programming contains blackout/restrictions. Carle, Figs. 2-3, ¶[0011]; Bacso, ¶¶[0086]-[0087];

Lin, ¶106. Thus, if an end user requests access to a particular content stream outside of blackout timing, without other reason, the content requester will receive the content, but when the local time for blackout begins, a POSITA would understand the originally requested stream will terminate. *See* Lin, ¶106.

8. Claim 9

a. [9.a]: "The computer-implemented method as in claim 1, wherein processing the reply from the subscription database comprises detecting that the end user is not a subscriber of the content publisher, the method further comprising: in a subscriber verification table, storing an entry indicating that the end user is not an authorized subscriber of the content publisher, and"

Fransdonk discloses or suggests [9.a] because it shows detecting that the end user is not a subscriber of the content publisher, including storing an entry in a subscriber verification table indicating that the end user is not an authorized subscriber of the content publisher. Lin, ¶107. For example, Fransdonk discloses that "the conditional access agent 28 interfaces with the conditional access server 36 to query subscriptions." Fransdonk ¶[0146]. And as explained for [1.c], the conditional access agent 28 queries the conditional access server 36 and subscription database "to validate subscriber content requests" based on access criteria. *E.g.*, Fransdonk, ¶¶[0062], [0098]. If the user is not a subscriber of the content, Fransdonk discloses displaying an error message to the user, including information on how to obtain a subscription. Fransdonk, ¶[0194]. Thus, Fransdonk discloses detecting whether a

user is a subscriber, including detecting that certain users are not subscribers. Lin, ¶¶107-08.

Moreover, the access criteria that conditional access agent 28 uses "are stored in such a way that retrieval can be performed efficiently" and are "organized by content provider and location." Fransdonk, ¶[0098]. Indeed, Fransdonk discloses storing information about subscribers in several tables in the subscription database. Fransdonk, ¶¶[0108]-[0133]. Fransdonk explains that the diagram in Fig. 4 shows the "real-time processes, databases and user interface that together provide[] the functionality of a conditional access server 36," (Fransdonk, ¶[0103]), including "a number of tables and fields … utilized by the conditional access server 36." Fransdonk, ¶[0108]. Fransdonk discloses various tables and their stored information, including the ACProfileSet table that represents "access criteria set (conditions) under which an item is provided to the subscriber" and includes a "SubscriptionFlag" binary entry. Fransdonk, ¶[0131].

A POSITA reading Fransdonk would have understood that Fransdonk's SubscriptionFlag would indicate whether the user was a subscriber of the content provider or was not a subscriber. Lin, ¶109. Storing binary information (e.g., whether a user is (TRUE) or is not (FALSE) has a subscription to view certain content) in data-structures was well-known in the art, and a POSITA would have understood Fransdonk's SubscriptionFlag to represent this binary distinction between whether

a user was or was not a subscriber, or at least would have found it obvious to do so. Chatani, ¶[0020]; Bacso, Table 1, ¶¶[0059]-[0060]; Lin, ¶109. A POSITA would have been motivated to store such basic data states in an easily accessible and searchable data structure, as taught by Fransdonk, about whether or not a user holds a subscription, because such storage means were well-known in the art, Fransdonk already discloses the means for storing such information, and a skilled artisan would have recognized the benefits of being able to easily access such information. *See* Fransdonk, ¶[0098] ("The access criteria are stored in such a way that retrieval can be performed efficiently…."); Lin, ¶109.

As Dr. Lin explains, it was well known to provide notifications to end users over a streaming network when a request for content failed, as Fransdonk expressly discloses. Lin, ¶110 (citing Fransdonk, ¶[0194]). Storing information about a user's subscription status would improve Fransdonk's error messaging means by incorporating a simplified check of the ACProfileSet Table for generating notifications within the system or to end users regarding end users that do not hold the subscriptions necessary to view certain content. Lin, ¶110. Indeed, Fransdonk discloses that "the conditional access agent 28 interfaces with the conditional access server 36," which stores the ACProfileSet table, "to query subscriptions." Fransdonk ¶[0146]. A POSITA would have found it straightforward to implement an IF/THEN logical comparison based on such queries to generate the types of notifications that

Fransdonk discloses based on the binary field of the subscription status housed in the ACProfileSet Table. Bi, Figs. 48-50, ¶¶[0189]-[0190]; Lin, ¶110. The technique lends to easy data structure management for the state of user subscriptions without adding additional complexities to the data structure storing such information. Lin, ¶110. Fransdonk's teaching the need to protect and secure media content provides a motivation by adding simple logic to the data structure that contributes to this stated goal. *See* Lin, ¶110; Fransdonk, ¶[0010]; *see also* '778 patent, 1:36-44.

b. [9.b]: "wherein transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream comprises: specifying in the notification that the end user is not an authorized subscriber of the content publisher from which the end user had requested delivery of the video stream."

Fransdonk discloses or suggests [9.b] as explained in section [1.d.i]. Lin, ¶111.

9. Claim 10: "The computer-implemented method as in claim 1, wherein processing the reply from the subscription database comprises detecting that the end user is a subscriber of the content publisher, the method further comprising: in a subscriber verification table, storing an entry indicating that the end user is an authorized subscriber of the content publisher."

Fransdonk discloses or suggests claim 10. Lin, ¶112.

As explained for [9.a], Fransdonk discloses storing information about the subscriber, including "access criteria" such as a "SubscriptionFlag" that includes a binary entry indicating whether a user is a subscriber. Fransdonk, ¶¶[0108]-[0133];

supra Section VI.A.8.a ([9.a]). As further described above in Section VI.A.8.a ([9.a]), a POSITA would have understood that a binary entry as True indicates a user is an authorized subscriber. Lin, ¶113.

10. Claim 11

a. [11.a]: "The computer-implemented method of claim 10 further comprising: receiving a second request from a second end user for delivery of the video stream to the second end user;"

[11.b]: "processing the second request to determine that the second end user is authorized to receive delivery of the video stream; and"

Fransdonk discloses or suggests [11.a] and [11.b]. Lin, ¶114.

As explained for limitations [1.a] and [1.c], Fransdonk discloses the "receiving" and "processing" limitations. Fransdonk teaches its system having a content distributor 20 that is equipped to receive requests from multiple users (i.e., a second request from a second end user). Fransdonk, ¶[0055]. Fransdonk receives requests from multiple users in the same manner for each user (i.e., processes a second request to determine authorization for a second user to view a specific content). Fransdonk, ¶¶[0060]-[0061]; Lin, ¶115. This content is processed such that a single piece of content (e.g., a live broadcast) can be viewed by many users. Fransdonk, ¶¶[0055], [0262].

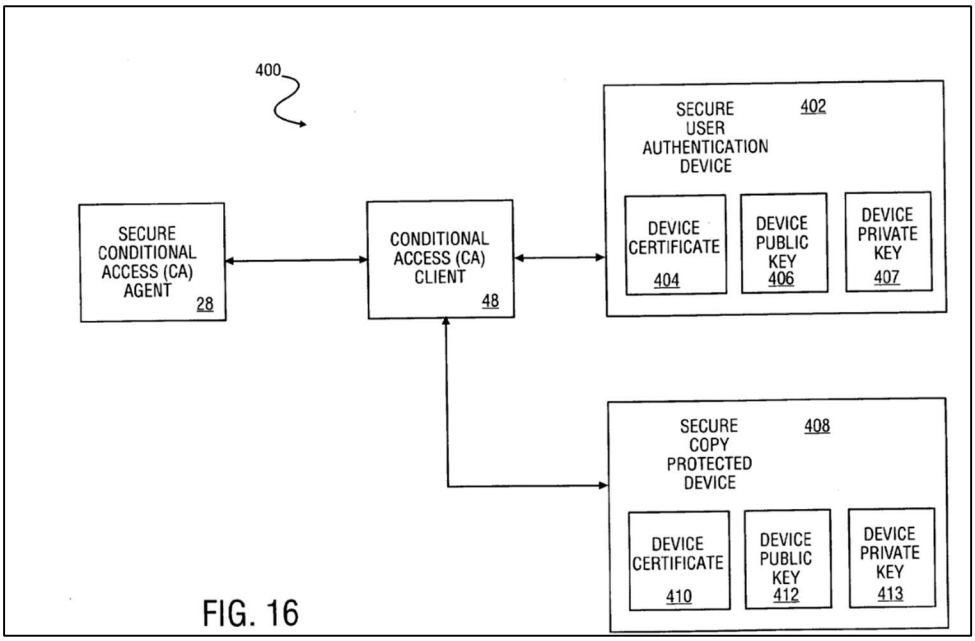
b. [11.c]: "initiating delivery of the video stream to the second user."

Fransdonk discloses or suggests [11.c] as explained for [1.d.ii]. Lin, ¶115.

11. Claim 12

a. [12.a]: "The computer-implemented method of claim 11, wherein processing the second request to determine that the second end user is authorized to receive delivery of the video stream comprises: determining that the second end user is the same as the end user; and"

Fransdonk discloses or suggests [12.a]. Lin, ¶116. Fransdonk recognizes that current hardware solutions tie the user to a specific device, limiting a user's ability to send requests to view content from alternative devices. Fransdonk, ¶[0331]. Fransdonk solves this issue by segmenting user authentication functionality from the content security functionality. Fransdonk, ¶[0332]; *see also id.*, Fig. 16.



Fransdonk, Fig. 16.

This segmenting provides users the ability to make requests from multiple devices for the same content. Fransdonk, ¶[0332]; Lin, ¶117. Fransdonk also teaches caching transactions so that the system can recognize a second request "from the same end user" such that a subscriber can watch certain content (e.g., a movie) multiple times without being charged for any repeated viewing as long as the content's viewed during the checkout/payment period described. Fransdonk, ¶[0138].

b. [12.b]: "in response to querying the subscriber verification table, determining that the second end user is an authorized subscriber of the content publisher."

Fransdonk discloses or suggests claim [12.b] as explained for claim 10. Lin, ¶118.

12. Claim 14: "The computer-implemented method of claim 10 further comprising: in the subscriber verification table, storing session information associated with the delivery of the video stream to the end user, wherein the session information is stored in accordance with a relative time at which the request from the end user was received."

Fransdonk discloses or suggests the additional limitations of claim 14 because it discloses that the conditional access agent 28 creates an "order request" that includes "user credentials, access criteria, and ***local time***" of the user's request for content and "stores this information[, e.g., the access criteria and local time,] together ***with the other session information***." Fransdonk, ¶[0175] (emphases added); *see also id.*, ¶¶[0153]-[0154], [0160]-[0176]; Lin, ¶119. For example, Fransdonk discloses that when a user selects and requests content from the system, (Fransdonk, ¶¶[0161]-[0164]), components of Fransdonk's conditional access agent 28 construct an order request using the "user credentials, access criteria, and local time" and "store[] this information together with the other session information." Fransdonk, ¶¶[0174]-[0175]; *see also id.*, ¶[0227] (discussing utilizing access criteria and session information when constructing an order request "based on a

current date and time" of the requested information). Fransdonk explains that the session information includes "access criteria, user credentials, local time, signature, etc." Fransdonk, ¶[0177]. Moreover, and as discussed above regarding claim 9, Fransdonk discloses that "access criteria" include additional information such as the fields shown in the ACProfileSet table. Fransdonk, ¶[0130]; Lin, ¶119. This includes information such as the SubscriptionFlag discussed above, as well as "Viewing time," time windows to start and stop blocking access, parental controls, etc. *Id.* Fransdonk's disclosure of storing the "local time" at which a request is made by the user and an order request that is generated with its "session information" thus discloses "storing session information associated with the delivery of the video stream to the end user . . . in accordance with a relative time at which the request from the end user was received," as claimed. Lin, ¶119.

Moreover, Fransdonk discloses that the "session information" includes "access criteria," which is stored in the ACProfileSet table, and thus discloses that the session information is stored "in the subscriber verification table," as claimed. Lin, ¶120. To the extent it is argued that Fransdonk discloses storing the session information in multiple tables, it would have been obvious to combine this data into a single subscriber verification table. Lin, ¶120. Storing data like Fransdonk's "session information" and/or "access criteria" was routine long before the effective date of the '778 patent. Lin, ¶120. Moreover, consolidating data from two or more

tables into one table was well known to POSITAs. Lin, ¶120. Indeed, a POSITA would have been motivated and found it obvious to combine such data into a single table to improve the speed with which the data could be accessed for queries or editing because storing data in one table would require fewer database calls than if the data were distributed across multiple tables. Lin, ¶120.

13. Independent Claim 15

a. [15.pre]: "A computer-implemented method for authorizing delivery of a video stream to an end user, the video stream being provided by a content source associated with a content publisher, the method comprising:"

To the extent limiting, Fransdonk discloses [15.pre] for the reasons explained for [1.pre]. Lin, ¶121.

b. [15.a]: "receiving a request from the end user for delivery of the video stream to the end user across a network;"

Fransdonk discloses or suggests [15.a] for the reasons explained for [1.a]. Lin, ¶122.

c. [15.b]: "querying a subscription database associated with the client publisher;"

Fransdonk discloses or suggests [15.b] for the reasons explained for [1.b]. Lin, ¶123.

d. [15.c]: "in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream;"

Fransdonk discloses or suggests [15.c] for the reasons explained for [1.c]. Lin, ¶124.

e. [15.d]: "if the end user is determined to have authorization to receive delivery of the video stream, creating an entry in a subscriber verification table specifying that the end user is an authorized subscriber of the content publisher, wherein the entry further specifies session information associated with delivery of the video stream to the end user, the session information being stored in accordance with a relative time at which the request from the end user was received; and"

Fransdonk discloses or suggests [15.d] for the reasons explained for claim 14. Lin, ¶125.

f. [15.e]: "initiating delivery of the video stream to the end user."

Fransdonk discloses or suggests [15.e] for the reasons explained for [1.d.ii]. Lin, ¶126.

14. Independent Claim 16

a. [16.pre]: "A system configured to authorize delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the system comprising:"

To the extent limiting, Fransdonk discloses or suggests [16.pre] for the reasons explained for [1.pre]. Lin, ¶127.

b. [16.a]: "a network;"

Fransdonk discloses [16.a] because it discloses a "method and system to . . . deliver content in a geographically controlled manner ***via a network*.**" Fransdonk, Title, Abstract, ¶[0052]; *see also id.*, ¶[0022]; Lin, ¶128. Likewise, Fransdonk teaches a content requester may provide for delivery of the video stream "via a network to the content destination." Fransdonk, Abstract, ¶[0371]; *see also id.*, ¶¶[0008], [0041], [0054]-[0057], [0214], [0217], [0394], Figs. 1, 2, 17, 24.

c. [16.b]: "a subscription database accessible via the network;"

Fransdonk discloses or suggests [16.b]. Lin, ¶129. Fransdonk discloses "a subscription database" because, as explained for [1.b], conditional access server is comprised of a number of "processes, ***databases,*** and user interfaces[.]" Fransdonk, ¶[0028], Fig. 3. The systems and methods taught by Fransdonk occur by verifying content stored in the various tables of the conditional access server (i.e., "accessible via the network") to relay the results of the query to an end user that requested content. *See* Fransdonk, ¶¶[0175] ("The order requested is also registered with the secure agent 88, which ***stores this information together with the other session information***."), [0123] ("SubscriptionForm" table); *see also id.* ¶¶[0106]-[0107], [0153]-[0154], [0227], Figs. 3, 4, 6B, 10A; Lin, ¶129.

d. [16.c]: "a content server configured to receive a request from the end user for delivery of the video stream to the end user across the network;"

Fransdonk discloses or suggests [16.c] for the reasons explained for [1.a]. Lin, ¶130.

e. [16.d]: "wherein the content server is configured to query the subscription database associated with the content publisher;"

Fransdonk discloses or suggests [16.d] for the reasons explained for [1.b]. Lin, ¶131.

f. [16.e]: "wherein the content server is further configured to process a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream; and"

Fransdonk discloses or suggests [16.e] for the reasons explained for [1.c]. Lin, ¶132.

g. [16.f.i]: "wherein the content server is configured to perform at least one of: transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and"

Fransdonk discloses or suggests [16.f.i] for the reasons explained for [1.d.i]. Lin, ¶133.

h. [16.f.ii]: "initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream."

Fransdonk discloses or suggests [16.f.ii] for the reasons explained for [1.d.ii]. Lin, ¶134.

15. Claim 17

a. [17.a]

Fransdonk discloses or suggests [17.a] for the reasons explained for [4.a]. Lin, ¶135.

b. [17.b]

Fransdonk discloses or suggests [17.b] for the reasons explained for [4.b]-[4.c]. Lin, ¶136.

c. [17.c]

Fransdonk discloses or suggests [17.c] for the reasons explained for claim 5. Lin, ¶137.

16. Claim 18

a. [18.a]

Fransdonk discloses or suggests [18.a] for the reasons explained for claim 6. Lin, ¶138.

b. [18.b]

Fransdonk discloses or suggests [18.b] for the reasons explained for claim 8. Lin, ¶139.

17. Claim 19

a. [19.a]

[19.b]

Fransdonk discloses or suggests [19.a] and [19.b] for the reasons explained for claim limitation [15.d] and claim [14]. Lin, ¶140.

18. Claim 20

a. [20.a]

Fransdonk discloses [20.a] for the reasons explained for [1.d.i] and [9.a]. Lin, ¶141.

b. [20.b]

Fransdonk discloses [20.b] for the reasons explained for [1.d.i] and [9.a]. Lin, ¶142.

c. [20.c]

Fransdonk discloses [20.c] for the reasons explained for [1.d.i] and [9.b]. Lin, ¶143.

B. Ground 2: Fransdonk in View of Norris Renders Obvious Claims 2, 3, and 13

1. Overview of the Combination

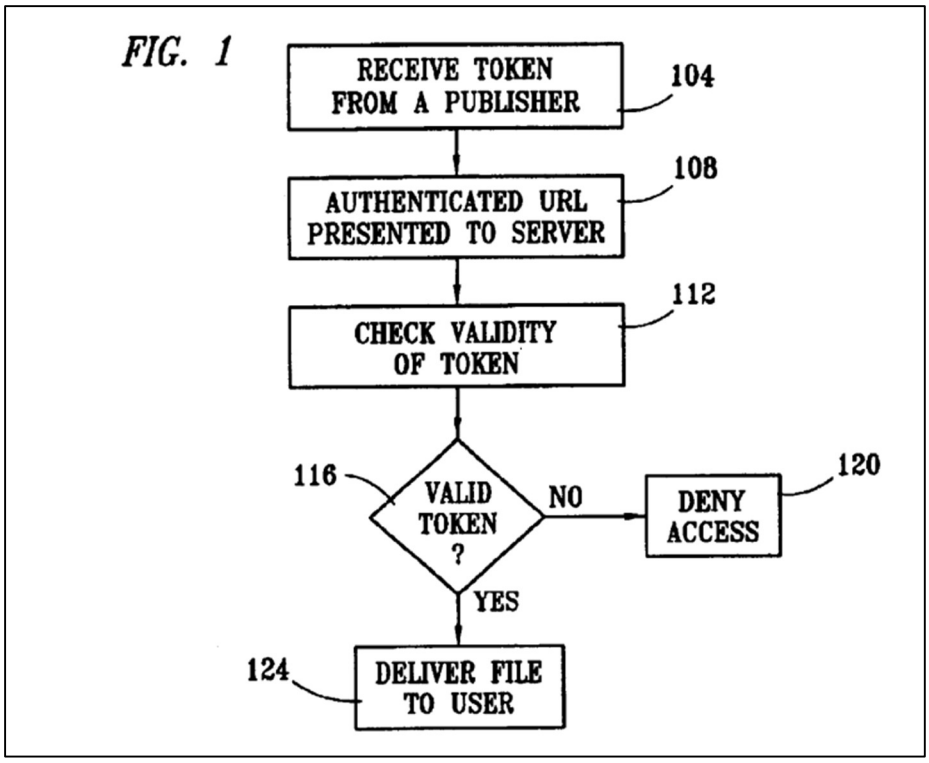
a. Norris

Norris discloses a system and method "for controlling access to content on a network computer." Norris, Title, Abstract. This includes audio/video and other multimedia content. Norris, 2:57-65, 1:14-18. The system and methods give content publishers the ability to control access to distributed content by using tokens to verify and authenticate a user's request for content. Norris, Abstract. A user may make a request that requires a content server to authenticate the user by processing a token and verifying its validity. Norris, 3:24-32. Norris describes a token as including different component fields that a content publisher can require to validate the token. Norris, 6:60-7:46, Table (below):

Bit Position	Component Indicated
0	IP Address
1	File path (sometimes referred to as the URL)
2	Password
3	Referer ID
4	Time Window
5	Unused
6	Unused
7	Unused
8	Unused

The ability to define the set of components needed for validation gives Norris's system flexibility based on what level of security it needs. Norris, 8:9-18. Figure 1 shows Norris's process for verifying the token, and if confirmed, delivering

the requested content. Norris, 4:4-8. If the token does not match, the token is "invalid," and the system denies access to the content and provides a message of "why access was denied." Norris, 4:8-12. This same method may work where a user acquires a "cookie" to authenticate a page and the content publisher "checks if the cookie is valid or not" before authenticating content (e.g., a URL). Norris, 5:20-25; Fig. 1.



Norris, Fig. 1.

Norris is analogous to the '778 patent because both are in the same field of endeavor: authenticating access requests to digital content. *Compare* Norris, Abstract ("A system and method for controlling access to content on a network computer.") *with* '778 patent, Abstract ("Embodiments generally disclosed herein

include computer-implemented methods for delivery of video content across a network…."); Lin, ¶¶55-57.

b. Combination of Fransdonk and Norris and Motivation to Combine

Fransdonk and Norris are similar. Lin, ¶144. Both describe systems and methods for authenticating digital content. *See, e.g.*, Fransdonk, Abstract, ¶¶[0021]-[0022]; Norris, Abstract, 1:46-2:31. And the goal of both disclosures is to combat content piracy or otherwise prevent unauthorized access to content. *Compare* Fransdonk, ¶¶[0009]-[0010] (explaining with the "widespread acceptance of the Internet as a distribution channel" also come "concerns regarding content piracy and digital rights management") *with* Norris, 1:34 ("A website publisher may wish to prevent piracy on its site.").

A POSITA would have found it obvious to use the token and cookie authentication techniques taught by Norris in the larger digital content authentication system of Fransdonk. Lin, ¶145. A POSITA would have been motivated to ensure Fransdonk's method for authentication provides the appropriate level of flexibility the system needs based on the security requirements for protecting its digital contents while maintaining its ability to distribute media. Lin, ¶145; *see* Fransdonk, ¶[0010] ("A challenge facing traditional pay media distributors is to enable content providers to control their proprietary content, while maintaining the flexibility to

distribute media content widely."). A POSITA would have used Norris's authentication means via tokens and cookies as an application of a known technique in Fransdonk's method because Norris's token authentication, which allows content publishers to define the set of components needed to authenticate specific content, provides the kind of flexible security Fransdonk contemplates for specific content publishers. *See* Norris, 7:29-46; Lin, ¶145.

Because Fransdonk and Norris both disclose systems and methods for authenticating digital video content, a POSITA would have had a reasonable expectation of success in implementing Norris's token authentication into Fransdonk's general system and method. Lin, ¶146. Furthermore, applying Norris's teaching to Fransdonk would have been a straightforward use of a known technique to enhance a similar device or method in the same manner. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417-18 (2017); Lin, ¶146.

2. Claim 2

a. [2.a]: "The computer-implemented method as in claim 1, wherein receiving a request from the end user comprises: receiving metadata from the end user;"

Fransdonk in view of Norris teaches [2.a]. Lin, ¶147.

Fransdonk teaches "receiving a request from the end user" for the reasons explained above in [1.a]. Norris teaches using means of authenticating a user's request for content with, at least, tokens and/or cookies. Norris, 3:56-63; 5:20-25. A

POSITA would have understood that tokens and cookies both comprise metadata. *See, e.g.*, Bi, ¶[0123]; Lin, ¶147. Indeed, claim 3 of the '778 patent expressly contemplates that the metadata would comprise a cookie or token. And Norris teaches tokens provided to users (e.g., a token embedded in a URL) subsequently get "presented to" a content server that receives the tokens to authenticate ("receiving metadata"). Norris, 3:11-16, 25-33.

b. [2.b]: "processing the metadata to identify a content publisher associated with the end user; and"

Fransdonk in view of Norris teaches [2.b]. Lin, ¶148.

Norris discloses "processing the metadata to identify a content publisher associated with the end user" because Norris teaches having tokens or cookies (metadata) generated at the content publisher's site. Lin, ¶148; Norris, 1:55-56 ("According to the present invention, a user initially receives a token from the publisher or the owner."). Norris explains tokens or cookies can be used in varied ways for authentication like through an authenticated URL link that checks if the metadata is valid or not. Norris, 4:19-33; 5:20-25; Lin, ¶148. Norris also discloses how it verifies the token ("processing the metadata") by, *inter alia*, extracting the components field from the token—referred to as "authentication information." Norris, 5:40-48. Norris then teaches the token may encode information such as authorizing publisher and/or the publisher passwords "to prevent a valid publisher

from using another publisher's content" as well as the user's IP address "to restrict access to content to specific users authorized by the publisher." Norris, 7:49-64; *see also id.*, 8:57-60; Lin, ¶148.

c. [2.c]: "determining whether the content publisher associated with the video stream is the same as the content publisher associated with the end user."

Fransdonk in view of Norris teaches [2.c]. Lin, ¶149.

Norris discloses providing secured access to restricted contents like pay-per-view movies, where content such as "graphics, movies or audio" may be linked via some third-party website. Norris, 3:39-44. Norris explains that a content publisher may engage a separate entity to host content while retaining control over access to such content. Norris, 3:5-10. So, tokens generated by Norris will ensure that the token generated for any user (content publisher associated with the end user) aligns with the access requirements of the digital content (content publisher associated with the video stream). *See* Norris, 4:19-33; Lin, ¶149. Further, as explained for [2.c] in Ground 1, Norris's token encoding captures such information like "authorizing publisher and/or the publisher passwords "to prevent a valid publisher from using another publisher's content" as well as the user's IP address "to restrict access to content to specific users authorized by the publisher." Norris, 7:49-64; *see also id.*, 8:57-60; Lin, ¶149. This information provides authentication for both a user's access rights and a publisher's access rights. *See id.*; Lin, ¶149.

As explained above, a POSITA would have found it obvious to use Norris's authentication means in Fransdonk's system. Lin, ¶150.

3. Claim 3: "The computer-implemented method as in claim 2, wherein the metadata is at least one of a token and a cookie."

Fransdonk in view of Norris teaches claim 3 because Norris expressly states it authenticates users' request for content via tokens and/or cookies. *See* Norris 2:23-31, 3:56-63; 4:15-32, 5:20-25, 6:9-13, 7:49-8:8; Lin, ¶151. As described for [2.a] *supra*, a POSITA would have understood that tokens and cookies both comprise metadata. Lin, ¶151.

As explained above, a POSITA would have found it obvious to use Norris's authentication means in Fransdonk's system. Lin, ¶151.

4. Claim 13: "The computer-implemented method of claim 11, wherein processing the second request to determine that the second end user is authorized to receive delivery of the video stream includes analyzing at least one of a token and a cookie, wherein the at least one of a token and a cookie is associated with the second request received from the second end user."

Fransdonk in view of Norris teaches claim 13. Lin, ¶152.

As discussed for claim 11 in ground 1 *supra*, Fransdonk contemplates multiple users, and therefore, discloses or suggests these limitations. *See* Section VI.A.10.a; Lin, ¶152. Norris explains that it performs user authentication with tokens and/or cookies. *See, e.g.*, Norris 3:56-63; 5:20-25. Norris's system and method

contemplates receiving multiple requests from multiple users because it provides control access for content "on a distributed network, i.e., ***multiple computers storing and providing access*** to the content." Norris, Abstract; *see also id.*, 3:25-28 ("A content server…has the ability to receive ***requests*** for content and can deliver content to ***users***."). Likewise, Norris teaches associating a second request received from a second end user because Norris discloses comparing bit-fields that include, among other components indicated, a user's IP Address. Norris, 7:49-53; *see also id.*, 7:1-13 (table):

Bit Position	Component Indicated
0	IP Address
1	File path (sometimes referred to as the URL)
2	Password
3	Referer ID
4	Time Window
5	Unused
6	Unused
7	Unused
8	Unused

Norris, 7:1-13 (table) (annotated).

The token encoding incorporation of a user's IP Address "allows the publisher to restrict access to content to specific users authorized by the publisher." Norris, 7:49-53. This individualized encoding allows individual requests (i.e., a second request) to be associated with the appropriate requesting user (i.e., a second user).

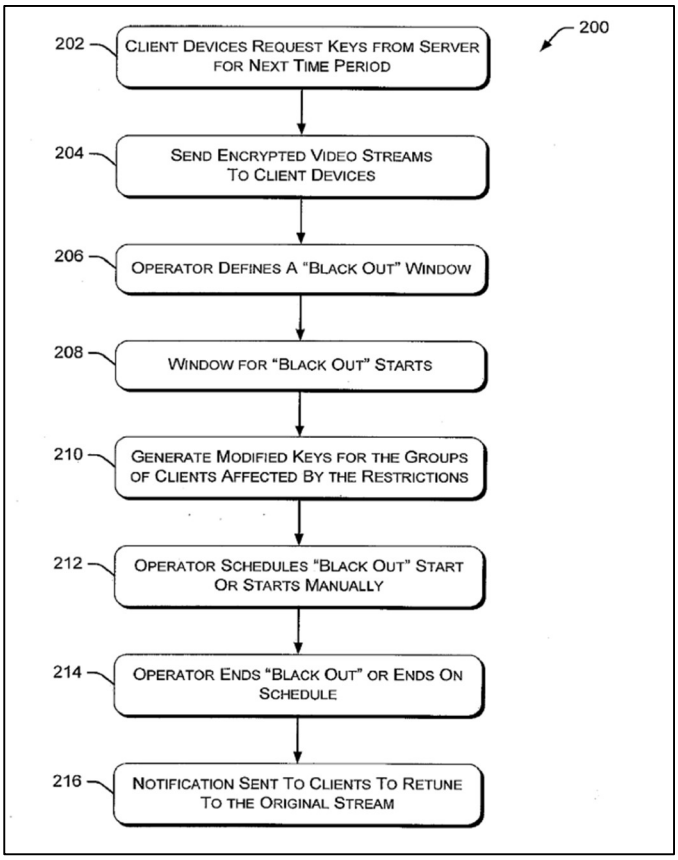
See id.; Lin, ¶153. As explained above, a POSITA would have found it obvious to use Norris's authentication means in Fransdonk's system. Lin, ¶153.

C. Ground 3: Fransdonk in View of Carle Renders Obvious Claims 4-8

1. Overview of the Combination

a. Carle

Carle discloses a method and systems for providing programmatic substitutions into video streams. Carle, ¶¶[0001], [0011]. Carle teaches making content substitutions based on certain geographic information where content may or may not be able to be viewed like, e.g., a "blacked out" region for certain events. Carle, ¶[0001]. Carle captures different geographic information such as a user's ZIP code, postal address, and geographic region code. Carle, ¶[0024]. This geographic information is used when determining if certain blackout windows occur, where the system will compare the geographic information of the user against the geographic blackout information received from content distributors to determine which users are affected by the restrictions. *See* Carle, Fig. 2; Lin, ¶58.



Carle, Fig. 2.

Carle is analogous to the '778 patent because they are in the same field of endeavor: authenticating access requests to stream content. *Compare* Carle, ¶[0004] ("The systems and methods described herein distribute keys to multiple clients. The keys are used by the clients to gain access to media content.") *with* '778 patent, Abstract ("Embodiments generally disclosed herein include computer-implemented methods for delivery of video content across a network…."); Lin, ¶59.

b. Combination of Fransdonk with Carle and Motivation to Combine

Fransdonk and Carle are similar. Lin, ¶154. Both describe systems and methods for authenticating streaming content. *See, e.g.*, Fransdonk, Abstract, ¶¶[0021]-[0022]; Carle, ¶¶[0013], [0020], [0025], Fig. 2. And a goal of both disclosures is to create cost-efficient means of handling content distribution. *Compare* Fransdonk, ¶[0016] ("A scalable key distribution system may become critical to distribute content associated with large-scale live events") *with* Carle, ¶[0002] ("[I]t would be desirable to provide a system that is capable of substituting content without requiring the use of many expensive, special-purpose [equipment].").

Although Fransdonk teaches considering geographic location in its content distribution system generally, to the extent Fransdonk does not expressly disclose restricting live-streaming delivery of content based on black out rules and timing requirements, Carle does. A POSITA would have understood that time and geographic restrictions for channel-based or program-based content were well-known components in streaming systems that were useful for facilitating authentication services between client devices and content publishers. *See* Bacso, ¶[0084] ("Location information can be stored … for blackouts."), ¶[0087]; *see also* Risan, Abstract, ¶[0011]; Bi, ¶¶[0165]-[0166]; Lin, ¶155.

For example, Carle teaches the use of program substitution based on geographic information about individual users to avoid the need for media systems to invest in special-purpose, expensive hardware. Carle, ¶¶[0002]-[0003]. A POSITA would have found it obvious to supplement the geographic authentication techniques taught by Fransdonk with those disclosed by Carle that expressly disclose blacking out content for certain regions during certain time periods. Lin, ¶156. A POSITA would have used Carle's geographic authentication means as an application of a known technique to supplement Fransdonk's method that already considers geographic restrictions because Carle's geographic authentication would provide the kind of cost-effective, scalable solution that would help monitor distributing content across a network that Fransdonk teaches and would ensure that content is not distributed to blacked out regions during blacked out times. Carle, ¶[0002]; Lin, ¶156. Likewise, a POSITA would have been motivated to integrate Carle's blackout disclosures into Fransdonk's system by placing it in the existing Subscription and Access Criteria Tables. Fransdonk, ¶¶[0121], [0124]; Carle, ¶[0033]; Lin, ¶156. Placing Carle's blackout information in the tables described above would enable easier communication between conditional access agent 28, conditional access server 36, and media client 49 for more seamless initiating and terminating transmissions based on access criteria restrictions. Carle, ¶[0025]; Lin, ¶156.

Because Fransdonk and Carle both disclose systems and methods for authenticating streaming content, a POSITA would have had a reasonable expectation of success in implementing Carle's geographic authentication into Fransdonk's general system and method. Lin, ¶157. Furthermore, applying Carle's teaching to Fransdonk would have been a straightforward use of a known technique to enhance a similar device or method in the same manner. Lin, ¶157.

2. Claim 4

a. [4.a]

Fransdonk in view of Carle teaches [4.a]. Lin, ¶158.

As explained for [4.a] in ground 1, Fransdonk discloses using proximity parameters specifying the geographic location of the end user. *See supra* Section VI.A.3.a; Lin, ¶158. Carle also discloses capturing geographic information ("proximity parameters") for groups of clients. Carle, ¶[0014]. Carle's system teaches monitoring live event updates for certain events such as blackout periods, whereby an event triggers program substitution based on the captured geographic information. Carle, ¶¶[0017], [0024]-[0025].

b. [4.b]-[4.c]

Fransdonk in view of Carle teaches [4.b] and [4.c]. Lin, ¶159.

As explained for [4.b] and [4.c] in Ground 1, Fransdonk discloses restricting delivery of the video stream if the user is in a geographic area not authorized to receive it. *See supra* Section VI.A.3.b.

Carle also discloses this limitation. Lin, ¶160. After an event triggers program substitution, Carle teaches processing a user's geographic information (proximity parameters) to determine whether to substitute programs. Carle, ¶[0024]. If the user's geographic information is included in an affected event, the event may be a blackout period where a user cannot view content (i.e., not authorized to receive [a] video stream). *See* Carle, ¶[0026] ("The 'black out' window defines the clients or groups of clients that ***are not permitted to access*** the restricted content."). Carle teaches "restricting the delivery of the video stream to the end user" because it blocks access to the restricted content during the designated blackout window. Carle, ¶[0027]; Lin, ¶160. Thus, a POSITA would have found it obvious to use Carle's geographic authentication means to supplement Fransdonk. Lin, ¶161.

3. Claim 5

Fransdonk in view of Carle teaches claim 5. Lin, ¶162.

As explained for Ground 1, Fransdonk discloses comparing the time of the receipt of the user's request to blackout times for requested content based on the location of the user. *See supra* Section VI.A.4.

To the extent it is argued Fransdonk does not disclose this limitation, Carle does. Lin, ¶163. Carle teaches that its system provides predetermined times for when content may not be available to users in certain geographic regions, such as for a particular sporting event. Carle, ¶¶[0002], [0004]. When a user makes a request during the blackout period for a restricted event ("relative time"), Carle discloses referencing the blackout period and the user's geographic information to determine whether to grant a user's request to access the restricted content. Carle, ¶¶[0026]-[0027]. Thus, a POSITA would have found it obvious to use Carle's geographic authentication means to supplement Fransdonk. Lin, ¶164.

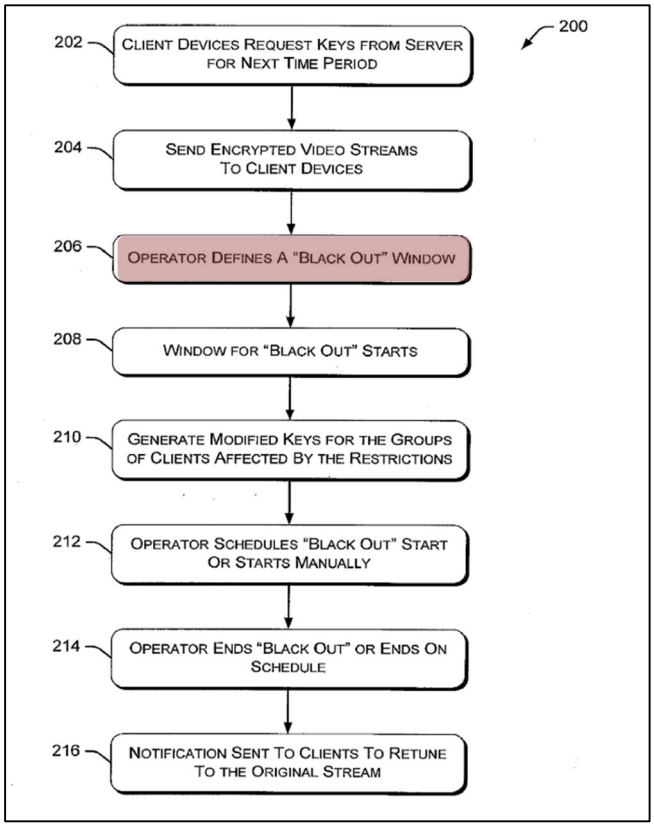
4. Claim 6

Fransdonk in view of Carle teaches claim 6. Lin, ¶165.

As explained for Ground 1, Fransdonk discloses comparing the time of the receipt of the user's request to blackout times for requested content based on the location of the user. *See supra* Section VI.A.5.

To the extent it is argued Fransdonk does not disclose this limitation, Carle does. Lin, ¶166. Carle teaches that its system provides predetermined times for when content may not be available to users in certain geographic regions, based on "black out" rules. Carle, ¶¶[0002], [0004], [0017]. When a user makes a request during the blackout period for a restricted event ("relative time"), Carle discloses referencing the blackout period and the user's geographic information to determine whether to

grant a user's request to access the restricted content. Carle, ¶¶[0026]-[0027]. Carle teaches associating the blackout rules with the content publisher because Carle gives the operator ("content publisher") the ability to define its own blackout rules. Carle, ¶[0027], Fig. 2.



Carle, Fig. 2 (annotated).

A POSITA would have found it obvious to use Carle's geographic authentication means to supplement Fransdonk. Lin, ¶167.

5. Claim 7

Fransdonk in view of Carle teaches claim 7. Lin, ¶168.

As explained for Ground 1, Fransdonk discloses restricting delivery based on subscription parameters for a particular group and member, including time and geographic criteria. *See supra* Section VI.A.6.

To the extent it is argued Fransdonk does not expressly disclose this limitation, Carle does. Lin, ¶169. Carle teaches that its system provides predetermined times for when content may not be available to users in certain geographic regions, such as for a particular sporting event. Carle, ¶¶[0002], [0004]. Carle discloses applying its geographic authentication means to group clients based on, "for example, geographic region, content to which the clients ***are subscribed***." Carle, ¶[0011]. Carle uses geographic information to determine whether a certain subscriber has rights to view specific programs. Carle, ¶[0020]. A POSITA would have found it obvious to use Carle's geographic authentication means to supplement Fransdonk. Lin, ¶170.

6. Claim 8

Fransdonk in view of Carle teaches claim 8. Lin, ¶171.

As explained for Ground 1, Fransdonk suggests terminating an initiated stream if a user is in a restricted geographic area. *See supra* Section VI.A.7.

To the extent it is argued Fransdonk does not expressly disclose this limitation, Carle does. Lin, ¶172. Carle teaches that its system provides predetermined times for when content may not be available to users in certain

geographic regions, such as for a particular sporting event. Carle, ¶¶[0002], [0004]. These predetermined windows will start and stop a user's feed for original content and provide "alternative content" at the appropriate start window, thus "terminating the delivery" of the "already-been initiated" video stream. *See* Carle ¶¶[0042]-[0043]. A POSITA would have found it obvious to use Carle's geographic authentication means to supplement Fransdonk. Lin, ¶173.

D. Ground 4: Fransdonk in View of Foti Renders Obvious Claims 9-12

1. Overview of the Combination

a. Foti

Foti discloses systems and methods for updating channel filtering information within the context of streaming media systems. Foti (Ex. 1013), Abstract, ¶¶[0001], [0007]; Lin, ¶60. Foti explains that channel filtering information may include both "whitelists" and "blacklists." Foti, ¶[0005]. As an example, Foti describes a "subscriber whitelist" that includes the "authorized broadcast channels that a consumer premise equipment (CPE), e.g., a set-top box or TV, is currently authorized to access from a service provider." *Id.* On the other hand, a blacklist may include the "list of confirmed unacceptable items" within the larger group. *Id.* While Foti provides a detailed discussion of channel filtering in the context of whitelists, it makes clear that this discussion applies equally to blacklists. *See* Foti, ¶[0006]. Foti further discloses that the whitelists (and thus the blacklists) allow the service

provider to provide "a subscriber [with] access [to] any channel or service he or she has subscribed to while blocking unauthorized . . . channels." Foti, ¶[0027].

Foti is analogous to the '778 patent because they are in the same field of endeavor: authenticating access requests to stream content. *Compare* Foti, ¶[0006] ("[T]he phrase 'subscriber whitelist' can be considered to be the list of authorized broadcast channels that a consumer [device]… is currently authorized to access from a service provider."); ¶[0026] ("The DSLAM 304 verifies whether the selected channel is authorized for this particular subscriber using the channel filtering information….") *with* '778 patent, 29:14-18 ("[I]f the end user is determined to have authorization to receive delivery of the video steam, the authorization manager 1850 creates an entry in a subscriber verification table…."). Lin, ¶61.

b. Combination of Fransdonk with Foti and Motivation to Combine

Fransdonk and Foti are similar. Lin, ¶174. Both describe systems and methods for authenticating streaming content. *See, e.g.*, Fransdonk, Abstract, ¶¶[0021] [0022]; Foti, ¶¶[0006]-[0007], [0026]. And goals for both disclosures is to create cost-efficient means of handling content distribution. *Compare* Fransdonk, ¶[0016] ("A scalable key distribution system may become critical to distribute content associated with large-scale live events") *with* Foti, ¶[0008] ("[E]xemplary embodiments

described below address the need for improving the efficiency of updating the channel filtering information.…"); Lin, ¶174.

Although Fransdonk teaches querying and updating subscription information generally, Foti discloses additional implementation details for querying and processing subscription information, including on a per-subscriber basis, using whitelists and blacklists. A POSITA would have understood that storing content-based restrictions in the form of whitelists and blacklists, as taught by Foti, would improve Fransdonk's disclosed authentication services between client devices and content publishers. *See, e.g.*, Foti, ¶¶[0005], [0007], Fig. 1; Trimper (Ex. 1017), 12:36-13:5, 14:60-64, Figs. 11-12; Lin, ¶175.

For example, Foti teaches prior to initiation of any content, its DSLAM 304 verifies whether the user is authorized to view the selected content. Foti, ¶[0026]. As disclosed, this initial provisioning allows subscribers to access any authorized channel while blocking unauthorized content, e.g., content for which the user is not a subscriber. Foti, ¶¶[0026]-[0027]. Foti's whitelist/blacklist is also updated over time as the user's subscriptions change. *Id.*; *see id.*, ¶[0007]. A POSITA would have found it obvious to supplement Fransdonk's subscriber information tables with additional subscription-level details provided by Foti that expressly disclose capturing whether or not a user is a subscriber of particular media content (i.e., is a subscriber of the content publisher). *See* Chatani, ¶[0020]; Bacso, Table 1,

¶¶[0059]-[0060]; Lin, ¶176. A POSITA would have used Foti's subscription-level whitelist/blacklist disclosures as an application of a known technique to supplement Fransdonk's method already considering subscriber information because Foti's subscription authentication means would provide the kind of cost-effective, scalable solution that would help preserve bandwidth across a network that Fransdonk teaches and seeks to implement. Foti, ¶[0008]; Lin, ¶176. A POSITA would have been motivated to integrate Foti's subscription whitelist/blacklist tables into Fransdonk system by placing it in the existing Subscription and Access Criteria Tables. Lin, ¶176; Fransdonk, ¶¶[0121], [0124]; Foti, ¶¶[0005]-[0007]. Placing Foti's subscription information in the tables described above would enable easier communication between conditional access agent 28, conditional access server 36, and media client 49 to seamlessly initiate and terminate transmissions based on access criteria restrictions. Lin, ¶176; Foti, ¶¶[0026]-[0027].

Because Fransdonk and Foti both disclose systems and methods for authenticating streaming content, a POSITA would have had a reasonable expectation of success in implementing Foti's subscription-level authentication means into Fransdonk's general system and method. Lin, ¶177. Furthermore, applying Foti's teaching to Fransdonk would have been a straightforward use of a known technique to enhance a similar device or method in the same manner. Lin, ¶177.

1. Claim 9

a. [9.a]

As discussed above in Section VI.A.8.a, Fransdonk discloses or renders obvious [9.a]. To the extent it is argued otherwise, the combination of Fransdonk and Foti discloses or renders obvious this limitation. Lin, ¶178. Foti discloses "detecting that the end user is not a subscriber of the content publisher [including] storing an entry indicating that the end user is not an authorized subscriber of the content publisher" because it discloses querying both "subscriber whitelist[s]" and "blacklists" to determine the end user is not authorized and updates (stores) this information in the whitelist/blacklist as the user's status changes. Lin, ¶178.

For example, as discussed above, Foti discloses a "subscriber whitelist" that includes the "the list of authorized broadcast channels that a consumer premise equipment (CPE), e.g., a set-top box or TV, is currently authorized to access from a service provider." Foti, ¶[0005]. It also discloses using a "blacklist," which is the converse of a "whitelist," and thus, discloses the channels that a consumer is not authorized to access certain content. Foti, ¶¶[0005]-[0006]. Foti further discloses that the whitelists (and thus the blacklists) allow the service provider to provide "a subscriber [with] access [to] any channel or service he or she has subscribed to while blocking unauthorized . . . channels," i.e., detecting that the user is not a subscriber. Foti, ¶[0027]; Lin, ¶179. The blacklist thus stores entries indicating whether or not

a user is a subscriber of particular media content (i.e., is a subscriber of the content publisher), as claimed. Lin, ¶179. This whitelist/blacklist subscription information is updated to maintain the accuracy of its authentication technique because an end user's subscriptions will change over time. Foti, ¶¶[0007], [0027].

Moreover, it would have been obvious to incorporate Foti's whitelist/blacklist information into Fransdonk's ACProfileSet table for the reasons discussed above. Lin, ¶180.

b. [9.b]

Fransdonk discloses or suggests [9.b] for the reasons explained in Ground 1 section [1.d.i]. Lin, ¶181.

2. Claim 10

As explained for [9.a], Fransdonk discloses storing information about the subscriber, including a "SubscriptionFlag" that includes a binary entry indicating whether a user is a subscriber or not. Fransdonk, ¶¶[0108]-[0133]; *supra* Section VI.A.8.a ([9.a]). As further described above in Section VI.A.8.a, a POSITA would have understood that a binary entry as True indicates a user is an authorized subscriber. Lin, ¶¶182-83.

To the extent Fransdonk does not expressly disclose this limitation, Foti does. Lin, ¶184. Foti discloses "storing an entry indicating that the end user is an authorized subscriber of the content publisher" because it provisions "channel

filtering information for a subscriber" to verify whether the user can view the requested content. Foti, ¶¶[0026]-[0027]. Foti's request includes provisioning subscriber-level information captured in the form of a whitelist. Foti, ¶[0006], Fig. 1. Foti discloses that a whitelist covers the subset of "confirmed acceptable items within a set or larger quantity of items," e.g., broadcast channels that an end user device ***are*** authorized to access from a service provider. Foti, ¶[0005]. This subscription information is updated to maintain the accuracy of its authentication technique because any particular end user's subscriptions will change over time. Foti, ¶[0027]; Lin, ¶184.

3. Claim 11

a. [11.a]

[11.b]

Fransdonk discloses or suggests [11.a] and [11.b] as explained in Ground 1 for [11.a] and [11.b]. Lin, ¶185.

b. [11.c]

Fransdonk discloses or suggests [11.c] as explained in Ground 1 for [1.d.ii]. Lin, ¶186.

4. Claim 12

a. [12.a]

Fransdonk discloses or suggests [12.a] as explained in Ground 1 for [12.a]. Lin, ¶187.

b. [12.b]

Fransdonk in view of Foti discloses or suggests claim [12.b] as explained for claim [10]. Lin, ¶188.

E. Ground 5: Claim 13 is Rendered Obvious by Fransdonk in View of Foti in Further View of Norris

1. Claim 13

As discussed for claim 11 in Ground 1, Fransdonk contemplates multiple users, and therefore, discloses or suggests these limitations. *See* Section VI.A.10.a. As explained above in Ground 2, a POSITA would have found it obvious to use Norris's authentication means in Fransdonk's system. *See* Section VI.B.4; Lin, ¶189. And as further discussed for claim 11 in Ground 4, to the extent Fransdonk does not disclose the subscription verification table required of claim 11, Foti does, and a POSITA would have been motivated to combine Foti with Fransdonk and Norris for the same reasons expressed in Ground 4. *See* Section VI.D.1.b; Lin, ¶189. Thus, the combination of Fransdonk in view of Foti in further view of Norris renders claim 13 obvious. Lin, ¶189.

VII. The Board Should Institute Review

A. 35 U.S.C. § 325(d)

The factors in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 at 17-18 (PTAB Dec. 15, 2017), favor institution. *See also Advanced*

Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH, IPR2019-01469, Paper 6 at 8-11 (PTAB Feb. 13, 2020) (precedential).

Advanced Bionics, step 1, and *Becton, Dickinson* factors (a), (b), and (d) favor institution because none of the references in this Petition were before the Office during prosecution. *See* Ex. 1002; '778 patent. The references are also not cumulative of the prosecution prior art because cited art teaches and renders obvious all challenged claims.

B. 35 U.S.C. § 314

The district court found the '778 patent claims ineligible under 35 U.S.C. § 101. Order GRANTING Defendant's Motion to Dismiss Counts II and IV of the Complaint, *Sandpiper CDN, LLC v. Google LLC*, No. 2:24-cv-03951 (C.D. Cal. Sept. 16, 2024), ECF No. 28 at 15. Sandpiper subsequently filed an amended complaint not asserting the '778 patent, but stating Sandpiper "reserves its right to appeal the Court's Order." First Amended Complaint for Patent Infringement, *Sandpiper CDN, LLC v. Google LLC*, No. 2:24-cv-03951 (C.D. Cal. Jan. 13, 2025), ECF No. 57 at 1, 28. Thus, any trial will not involve the '778 patent at least until after any appeal, causing the *Fintiv* factors to weigh strongly against discretionary denial.

Factor 1 favors institution because "the [district court's § 101] judgment has the same effect as a stay." *Wyze Labs, Inc. v. Sensormatic Elecs., LLC*, IPR2020-

01486, Paper 14 at 9-10 (PTAB Apr. 6, 2021); *accord Apple Inc. v. Geoscope Techs. Pte. Ltd.*, IPR2024-00255, Paper 14 at 13 (PTAB May 31, 2024). Because the district court invalidated the claims based on a "ground that could not have been raised before the Board, [this case] does not raise concerns of inefficient duplication of efforts or potentially inconsistent results." *Apple*, Paper 14, at 12. Likewise, the district court will not address any anticipation and obviousness issues involving the '778 patent (if it addresses them at all) before the Board's final written decision, removing any concerns about duplication of efforts. *Wyze Labs*, Paper 14 at 10. Moreover, Petitioner cannot delay filing this petition due to the 35 U.S.C. § 315(b) statutory bar. *See id.*

Factor 2 favors institution because any trial in the related litigation will not involve the '778 patent as Sandpiper has not asserted the '778 patent in its amended complaint.

Factor 3 favors institution because the Court and parties have expended few resources in litigation. Indeed, since the court's September 16, 2024 ruling that the claims were patent-ineligible, the parties have not expended resources involving the '778 patent, and any future resources will not involve the '778 patent.

Factor 4 favors institution because there is no overlap between issues raised here (§§ 102/103) and in the related proceeding (§ 101). "[The Board] cannot institute a trial in an *inter partes* review to determine whether the claims are directed

to eligible subject matter under § 101," making the patentability challenges in the petition "materially different from the legal issue considered by the [district] court." *Wyze Labs*, Paper 14 at 16. Thus, "this factor weighs heavily in favor of institution." *Id.*

Factor 5 favors institution because, despite Petitioner being the defendant in the parallel proceeding, any trial involving the '778 patent will occur well after a Final Written Decision as Patent Owner must first appeal and succeed in reversing the district court's § 101 judgment. *See Wyze Labs*, Paper 14 at 16.

Factor 6 favors institution. No other party has sought review of the '778 patent, minimizing any likelihood of serial or parallel petitions. Petitioner relies on prior art that the Office never applied, presents different invalidity grounds, and relies on Dr. Lin's declaration. *Supra*, §VII.A. The public interest against "leaving bad patents enforceable" supports institution. *Thryv, Inc v. Click-To-Call Techs., LP*, 140 S. Ct. 1367, 1374 (2020).

VIII. Mandatory Notices

A. Real Party-in-Interest

The Petitioner and real party-in-interest is Google LLC.[2]

B. Related Matters

Sandpiper asserted the '778 patent in the following litigation:

- *Sandpiper CDN, LLC v. Google LLC*, No. 2:24-cv-03951 (C.D. Cal. May 10, 2024).

[2] Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.

C. Lead and Back-Up Counsel, and Service Information

Lead Counsel	Back-up Counsel
Erika H. Arner (Reg. No. 57,540) erika.arner@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2700 Fax: 202-408-4400	Daniel C. Tucker (Reg. No. 62,781) daniel.tucker@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2700 Fax: 202-408-4400 Kara A. Specht (Reg. No. 69,560) kara.specht@finnegan.com Wyatt L. Bazrod (Reg. No. 81,776) wyatt.bazrod@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 271 17th Street, NW Suite 1400 Atlanta, GA 30363-6209 Tel: 571-203-2700 Fax: 404-653-6444 Cara R. Regan (Reg. No. 70,209) cara.regan@finnegan.com Sydney R. Kestle (Reg. No. 78,725) sydney.kestle@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue, NW Washington, DC 20001-4413 Tel: 202-408-6013 Fax: 202-408-4400

Petitioner consents to electronic service at the following email address: Google-Sandpiper-IPRs@finnegan.com.

IX. Grounds for Standing

Petitioners certify the ’778 patent is available for *inter partes review* and that Petitioners are not barred or estopped from requesting *inter partes review*.

X. Conclusion

Petitioner requests institution of *inter partes* review and cancellation of the challenged claims.

Respectfully submitted,

Dated: May 7, 2025

By: /Erika H. Arner/
Erika H. Arner (Reg. No. 57,540)

CLAIM APPENDIX

[1.pre] 1. A computer-implemented method for authorizing delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the method comprising:

[1.a] receiving a request from the end user for delivery of the video stream to the end user across a network;

[1.b] querying a subscription database associated with the content publisher;

[1.c] in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream; and

[1.d.i] performing at least one of:

transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and

[1.d.ii] initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription

database indicates the end user is authorized to receive delivery of the video stream.

[2.a] 2. The computer-implemented method as in claim 1, wherein receiving a request from the end user comprises:

receiving metadata from the end user;

[2.b] processing the metadata to identify a content publisher associated with the end user; and

[2.c] determining whether the content publisher associated with the video stream is the same as the content publisher associated with the end user.

[3] 3. The computer-implemented method as in claim 2, wherein the metadata is at least one of a token and a cookie.

[4.a] 4. The computer-implemented method as in claim 1 further comprising:

processing proximity parameters associated with the end user, wherein the proximity parameters specify a geographic location of the end user to where video content is transmitted;

[4.b] based on the processing of the proximity parameters, determining that the end user is not authorized to receive the video stream; and

[4.c] restricting delivery of the video stream to the end user.

[5] 5. The computer-implemented method as in claim 4, wherein determining that the end user is not authorized to receive the video stream comprises:

given a relative time associated with the receipt of the request from the end user, determining whether the video stream should be blacked out for at least a time period associated with the relative time in relation to the geographic location of the end user.

[6] 6. The computer-implemented method of claim 4, wherein restricting delivery of the video stream to the end user is in accordance with black out rules associated with the content publisher, the black out rules having associated time restrictions and geographic restrictions prescribed by the content publisher for the end user.

[7] 7. The computer-implemented method of claim 4, wherein restricting delivery of the video stream to the end user is in

accordance with subscription parameters of the content publisher for a group of end users, the subscription parameters including at least one of a time restriction and a geographic restriction, and wherein the end user is a member of the group of end users to which the subscription parameters apply.

[8] 8. The computer-implemented method as in claim 4, wherein restricting delivery of the video stream comprises:

terminating the delivery of the video stream to the end user if delivery of the video stream to the end user has already been initiated.

[9.a] 9. The computer-implemented method as in claim 1, wherein processing the reply from the subscription database comprises detecting that the end user is not a subscriber of the content publisher, the method further comprising:

in a subscriber verification table, storing an entry indicating that the end user is not an authorized subscriber of the content publisher, and

[9.b] wherein transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream comprises:

[9.c] specifying in the notification that the end user is not an authorized subscriber of the content publisher from which the end user had requested delivery of the video stream.

[10] 10. The computer-implemented method as in claim 1, wherein processing the reply from the subscription database comprises detecting that the end user is a subscriber of the content publisher, the method further comprising:

in a subscriber verification table, storing an entry indicating that the end user is an authorized subscriber of the content publisher.

[11.a] 11. The computer-implemented method of claim 10 further comprising:

receiving a second request from a second end user for delivery of the video stream to the second end user;

[11.b] processing the second request to determine that the second end user is authorized to receive delivery of the video stream; and

[11.c] initiating delivery of the video stream to the second user.

[12.a] 12. The computer-implemented method of claim 11, wherein processing the second request to determine that the second end user is authorized to receive delivery of the video stream comprises:

determining that the second end user is the same as the end user; and

[12.b] in response to querying the subscriber verification table, determining that the second end user is an authorized subscriber of the content publisher.

[13] 13. The computer-implemented method of claim 11, wherein processing the second request to determine that the second end user is authorized to receive delivery of the video stream includes analyzing at least one of a token and a cookie, wherein the at least one of a token and a cookie is associated with the second request received from the second end user.

[14] 14. The computer-implemented method of claim 10 further comprising:

in the subscriber verification table, storing session information associated with the delivery of the video stream to the end user, wherein the session information is stored in accordance with a relative time at which the request from the end user was received.

[15.pre] 15. A computer-implemented method for authorizing delivery of a video stream to an end user, the video stream being provided by a content source associated with a content publisher, the method comprising:

[15.a] receiving a request from the end user for delivery of the video stream to the end user across a network;

[15.b] querying a subscription database associated with the client publisher;

[15.c] in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream;

[15.d] if the end user is determined to have authorization to receive delivery of the video stream, creating an entry in a subscriber verification table specifying that the end user is an authorized subscriber of the content publisher, wherein the entry further specifies session information associated with delivery of the video stream to the end user, the session information being stored in accordance with a relative time at which the request from the end user was received; and

[15.e] initiating delivery of the video stream to the end user.

[16.pre] 16. A system configured to authorize delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the system comprising:

[16.a] a network;

[16.b] a subscription database accessible via the network;

[16.c] a content server configured to receive a request from the end user for delivery of the video stream to the end user across the network;

[16.d] wherein the content server is configured to query the subscription database associated with the content publisher;

[16.e] wherein the content server is further configured to process a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream; and

[16.f.i] wherein the content server is configured to perform at least one of:

transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and

[16.f.ii] initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream.

[17.a] 17. The system as in claim 16 further comprising:

proximity parameters associated with the end user, wherein the proximity parameters specify a geographic location of the end user to where video content is transmitted;

[17.b] wherein the content server is configured to process the proximity parameters to determine whether the end user is authorized to receive the video stream; and

[17.c] wherein a determination that the end user is not authorized to receive the video stream comprises:

given a relative time associated with the receipt of the request from the end user, determining whether the video stream should be blacked out for at least a time period associated with the relative time in relation to the geographic location of the end user.

[18.a] 18. The system as in claim 17 further comprising:

wherein the content server is configured to restrict delivery of the video stream to the end user in accordance with black out rules associated with the content publisher, the black out rules having associated time restrictions and geographic restrictions prescribed by the content publisher for the end user; and

[18.b] based on the black out rules, the content server is further configured to terminate the delivery of the video stream to the end user if delivery of the video stream to the end user has already been initiated.

[19.a] 19. The system as in claim 16 further comprising:

a subscriber verification table;

[19.b] if the end user is determined to be an authorized subscriber of the content publisher, the content server is configured to store an entry in the subscriber verification table indicating that the end user is an authorized subscriber of the content publisher, wherein the entry further includes session information associated with the delivery of the video stream to the end user, the session information being stored in accordance with a relative time at which the request from the end user was received.

[20.a] 20. The system as in claim 16 further comprising:

a subscriber verification table;

[20.b] if the end user is determined not to be an authorized subscriber of the content publisher, the content server is configured

to store an entry in the subscriber verification table indicating that the end user is not an authorized subscriber of the content publisher, and

[20.c] wherein the content server is configured to specify in the notification that the end user is not an authorized subscriber of the content publisher from which the end user had requested delivery of the video stream.

37 C.F.R. § 42.24(D) CERTIFICATION

Pursuant to 37 C.F.R. § 42.24(a)(1)(i), Petitioner certifies that this petition complies with the requirements of 37 C.F.R. § 42.24. Excluding parts of this Petition exempted under § 42.24(a), this Petition contains 13,840 words, as measured by the word-processing system used to prepare this paper.

Dated: May 7, 2025

/Erika H. Arner/
Erika H. Arner (Reg. No. 57,540)
Lead Counsel

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 8,595,778, the associated Power of Attorney, and Exhibits 1001-1017, were served on May 7, 2025, by FedEx Priority Overnight® on the correspondence address of record indicated in the Patent Office's Patent Center system for U.S. Patent No. 8,595,778.

ATTN: Patent Docketing
Level 3 Communications, LLC
931 14th St.
Denver, CO 80202

Dated: May 7, 2025

/Daniel E. Doku/
Daniel E. Doku
Senior Litigation Legal Assistant
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP