

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC, SAMSUNG ELECTRONICS AMERICA, INC., AND
SAMSUNG ELECTRONICS CO., LTD.,

Petitioners,

v.

TRUESIGHT COMMUNICATIONS LLC,

Patent Owner.

Case No. IPR2025-00025

U.S. Patent No. 8,949,879

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	PRECISE RELIEF REQUESTED	1
II.	THE '879 PATENT	1
III.	OVERVIEW OF PRIOR ART	3
	A. Sullivan.....	3
	B. Leung.....	7
	C. Craner	10
IV.	LEVEL OF ORDINARY SKILL IN THE ART	14
V.	CLAIM CONSTRUCTION	14
VI.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	14
	A. Claims 1-19 Are Obvious over Sullivan, Leung, and Craner	14
	1. Rationale for Combining Sullivan and Leung	14
	a. Combining Sullivan and Leung to implement a V-chip on Sullivan's PVR.....	15
	b. Combining Sullivan and Leung to implement access controls for digital content in a digital library on a per media and per user basis that overrides the default V-chip policy.....	19
	2. Independent Claim 1	26
	a. [1pre]: "An apparatus for setting rating based access controls for known digital content to be played on a video playback device having a V-chip, the apparatus comprising:"	26
	b. [1a]: "a rating policy management module for selectively setting rating based access control on a per media and per user basis for digital content of a digital library thereby	

	overriding a policy set by the V-chip for access to the digital content from the video playback device; and”	28
c.	[1b]: “a rating policy enforcement module for enforcing rating based access to the individual digital content for a plurality of users separate from and in addition to an administrator,”	30
d.	[1c]: “wherein at least a first user and a second user of the plurality of users have different media rating requirements and have different media ratings associated with a same specific digital content,”	31
e.	[1d]: “wherein a first of the two users is allowed to access the specific digital content based upon a first authentication code and a second of the two users is blocked from access to the specific digital content based upon a second authentication code,	33
f.	[1e]: “wherein the first authentication code comprises a personal identification number (PIN),”	34
g.	[1f]: “wherein the different ratings associated with the specific digital content are enforced using the first and second authentication codes, and”	36
h.	[1g]: “wherein the first of the two users is allowed to access the specific digital content in response to determining that a content identifier of the specific digital content matches a user identifier of the first user and the personal identification number of the first user is successfully authenticated.”	37
3.	Dependent Claims	40
a.	Claim 2: “The apparatus of claim 1, further comprising a rating policy database for storing rating based access controls for digital content of the digital library.”	40

b.	Claim 3: “The apparatus of claim 2, further comprising a data port for exporting the policy database to another playback device.”	41
4.	Independent Claim 4	43
a.	[4pre]: “A method in a computing system for creating specific rating policies for digital media access, the method comprising:”	43
b.	[4a]: “under control of the computing system having a memory and a processor, performing the acts of:”	43
c.	[4b]: “retrieving media information from the memory comprising a rating based media access policy for a digital content;” [4c]: “displaying the rating based media access policy to a user;”	44
d.	[4d]: “receiving from the user a first rating based access control policy override action for a first viewer and a second, different, rating based access control policy override action for a second viewer with respect to a same specific digital content,”	46
e.	[4e]: “wherein the first viewer and second viewer are separate and distinct from the user from which the override actions are received, and”	51
f.	[4f]: “wherein the first viewer is associated with a first authentication code unique to the first viewer and the second viewer is associated with a second authentication code unique to the second viewer;”	51
g.	[4g]: “storing the first and second policy override actions in a rating policy repository wherein future playback of the digital content is allowed or blocked consistent with the stored policy override action, and”	51
h.	[4h]: “wherein the first viewer is allowed to access the specific digital content based upon the first authentication code and the second viewer is blocked from access to the	

	specific digital content based upon the second authentication code,”	52
i.	[4i]: “wherein the first authentication code comprises a personal identification number (PIN), and”	54
	[4j]: “wherein the first of the two viewers is allowed to access the specific digital content in response to determining that a content identifier of the specific digital content matches a user identifier of the first viewer and the personal identification number of the first viewer is successfully authenticated.”	54
5.	Dependent Claims	54
a.	Claim 5: “The method of claim 4 further comprising validating the authentication codes of the first viewer and the second viewer.”	54
b.	Claim 6: “The method of claim 4, wherein the first and second authentication codes comprise a personal identification number (PIN).”	55
c.	Claim 7: “The method of claim 5, wherein the authentication codes comprise biometric information.”	55
d.	Claim 8: “The method of claim 4, further comprising displaying the media information, wherein the media information comprises a media rating.”	56
e.	Claim 9: “The method of claim 4, further comprising displaying the media information, wherein the media information comprises a media owner.”	60
f.	Claim 10: “The method of claim 4, wherein the first policy override action comprises modifying media access for the first viewer and the second policy override action comprises modifying media access for the second viewer.”	64

g.	Claim 11: “The method of claim 4, wherein the first policy override action comprises modifying media access for a group that includes the first viewer.”	65
6.	Independent Claim 12	66
a.	[12pre]: “A method in a computing system for rating based media access policy enforcement, the method comprising:”	66
b.	[12a]: “under control of a video playback device having a V-chip that specifies default rating based access policy, performing the acts of:”	66
c.	[12b]: “displaying metadata;”	66
d.	[12c]: “responsive to a first user selecting a media content from the displayed metadata, and responsive to determining that rating based access control configured to override the V-chip default rating based access policy is enabled:”	71
e.	[12d]: “reading media information”	73
f.	[12e]: “reading a default rating based access policy action associated with the selected media content configured to override the V-chip default rating based access policy; and”	73
g.	[12f]: “responsive to determining that an authentication code is required: validating an authentication code; and”	74
	[12g]: “beginning playback of the media; and”	74
h.	[12h]: “responsive to a second different user selecting the same media from the displayed metadata: determining that an authentication code associated with the second preventing playback of the media”	75
i.	[12i]: “wherein the first and second users are not administrators of the rating based access control	

configured to override the V-Chip default rating based access policy,”	76
[12j]: “wherein the first authentication code comprises a personal identification number (PIN), and”	77
[12k]: “wherein the first of the two users is allowed to access the media content in response to determining that a content identifier of the media content matches a user identifier of the first user and the personal identification number of the first user is successfully authenticated.”	77
7. Dependent Claims	77
a. Claim 13: “The method of claim 12, wherein the authentication codes comprise personal identification numbers.”	77
b. Claim 14: “The method of claim 12, wherein the authentication codes comprise biometric information.”	77
c. Claim 15: “The method of claim 12, wherein the default rating based access policy action is to deny access.”	78
d. Claim 16: “The method of claim 12, wherein the media information comprises a rating.”	78
e. Claim 17: “The method of claim 12, wherein the media information comprises a genre.”	78
f. Claim 18: “The method of claim 12, wherein the media information comprises a media owner.”	80
g. Claim 19: “The method of claim 12, further comprising retaining the associated authentication code of each user during a session associated with each user.”	81
VII. DISCRETIONARY DENIAL IS NOT WARRANTED.....	83
A. 35 U.S.C. § 314(a) Does Not Warrant Discretionary Denial.....	83
B. 35 U.S.C. § 325(d) Does Not Warrant Discretionary Denial	84

VIII. MANDATORY NOTICES	85
A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1).....	85
B. Related Matters Under 37 C.F.R. § 42.8(b)(2)	85
C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	86
D. Service Information Under 37 C.F.R. § 42.8(b)(4).....	87
IX. GROUNDS FOR STANDING.....	88
X. CONCLUSION.....	88

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020)	84, 85
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	83
<i>Arbutus Biopharma Corp. v. ModernaTX, Inc.</i> , 65 F.4th 656 (Fed. Cir. 2023)	69
<i>CoolIT Sys., Inc. v. Asetek Danmark A/S</i> , IPR2021-01195, Paper 10 (PTAB Dec. 28, 2021)	83
<i>NetNut Ltd. v. Bright Data Ltd.</i> , IPR2021-01492, Paper 12 (PTAB Mar. 21, 2022)	84
<i>Protect Animals with Satellites v. OnPoint Sys., LLC</i> , IPR2021-01483, Paper 11 (PTAB Mar. 4, 2022)	84
<i>Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	14
Statutes	
35 U.S.C. § 102 (pre-AIA)	3, 7, 10
35 U.S.C. § 103 (pre-AIA)	1
35 U.S.C. § 311	1
35 U.S.C. § 314(a)	83
35 U.S.C. § 325(d)	84

Regulations

37 C.F.R. § 42.8(b)(1)	85
37 C.F.R. § 42.8(b)(2)	85
37 C.F.R. § 42.8(b)(3)	87
37 C.F.R. § 42.8(b)(4)	89

Other Authorities

USPTO, Guidance Memo (June 21, 2022)	83
--------------------------------------	----

LIST OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 8,949,879 to Zipperer et al. (“the ’879 patent”)
Ex. 1002	File History of U.S. Patent No. 8,949,879
Ex. 1003	Expert Declaration of Henry Houh, Ph.D. (“Houh”)
Ex. 1004	Curriculum Vitae of Henry Houh, Ph.D.
Ex. 1005	U.S. Patent Application Publication No. 2005/0028191 to Sullivan et al. (“Sullivan”)
Ex. 1006	U.S. Patent Application Publication No. 2002/0095673 to Leung et al. (“Leung”)
Ex. 1007	U.S. Patent No. 8,079,044 to Craner (“Craner”)
Ex. 1008	Complaint for Patent Infringement from <i>Truesight Communications LLC v. Samsung Electronics Co. et al.</i> , No. 2:23-cv-00643-JRG, Dkt. 1 (E.D. Tex. Dec. 29, 2023)
Ex. 1009	Plaintiff Truesight Communications LLC’s Notice of Compliance with Service of Its P.R. 3-1 and 3-2 Infringement Contentions to Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc., from <i>Truesight Communications LLC v. Samsung Electronics Co. et al.</i> , No. 2:23-cv-00643-JRG, Dkt. 21 (E.D. Tex. May 30, 2024)
Ex. 1010	First Amended Docket Control Order from <i>Truesight Communications LLC v. Samsung Electronics Co. et al.</i> , No. 2:23-cv-00643-JRG, Dkt. 34 (E.D. Tex. June 28, 2024)
Ex. 1011	U.S. Patent No. 6,662,365 to Sullivan et al. (“Sullivan ’365”)
Ex. 1012	U.S. Patent Application Publication No. 2006/0277564 to Jarman (“Jarman”)

Ex. 1013	U.S. Patent Application Publication No. 2008/0232771 to Walls et al. (“Walls”)
Ex. 1014	U.S. Patent Application Publication No. 2006/0271791 to Novack et al. (“Novack”)
Ex. 1015	U.S. Patent Application Publication No. 2007/0214473 to Barton et al. (“Barton”)
Ex. 1016	U.S. Patent No. 6,477,705 to Yuen et al. (“Yuen”)
Ex. 1017	U.S. Patent No. 6,643,715 to Arthur (“Arthur”)
Ex. 1018	U.S. Patent Application Publication No. 2005/0160458 to Baumgartner (“Baumgartner”)

I. PRECISE RELIEF REQUESTED

Google LLC, Samsung Electronics America, Inc., and Samsung Electronics Co., Ltd. (collectively, “Petitioners”), request review under 35 U.S.C. § 311 of claims 1-19 (“challenged claims”) of U.S. Patent No. 8,949,879 (“the ’879 patent”) (Ex. 1001) and cancellation of the challenged claims based on the following unpatentability ground:

Ground	Claims	Basis	Prior Art
1	1-19	Pre-AIA 35 U.S.C. § 103	Sullivan, Leung, and Craner

II. THE ’879 PATENT

The ’879 patent describes access controls for content on playback devices. Ex. 1001, Title, 1:13-15. The ’879 patent purports to overcome problems with the V-chip, which conventionally prevented children from viewing content if its rating (e.g., PG-13) exceeded a rating policy configuration (e.g., block PG-13 and higher) set by a parent. *Id.*, 1:19-2:60. For example, the “single override” provided by a conventional V-chip’s PIN is purportedly “insufficient” in households with different-aged children because “the most restrictive rating policy must be implemented.” *Id.*, 2:9-20, 2:33-48. The program rating also “may not coincide with the parent’s judgments.” *Id.*, 2:49-60.

The '879 patent discloses a computing configuration with a digital library that allows multiple user authenticators and parental overrides of a program rating.

Id., 3:1-2, 5:5-6, 6:1-7:21, FIG. 2.

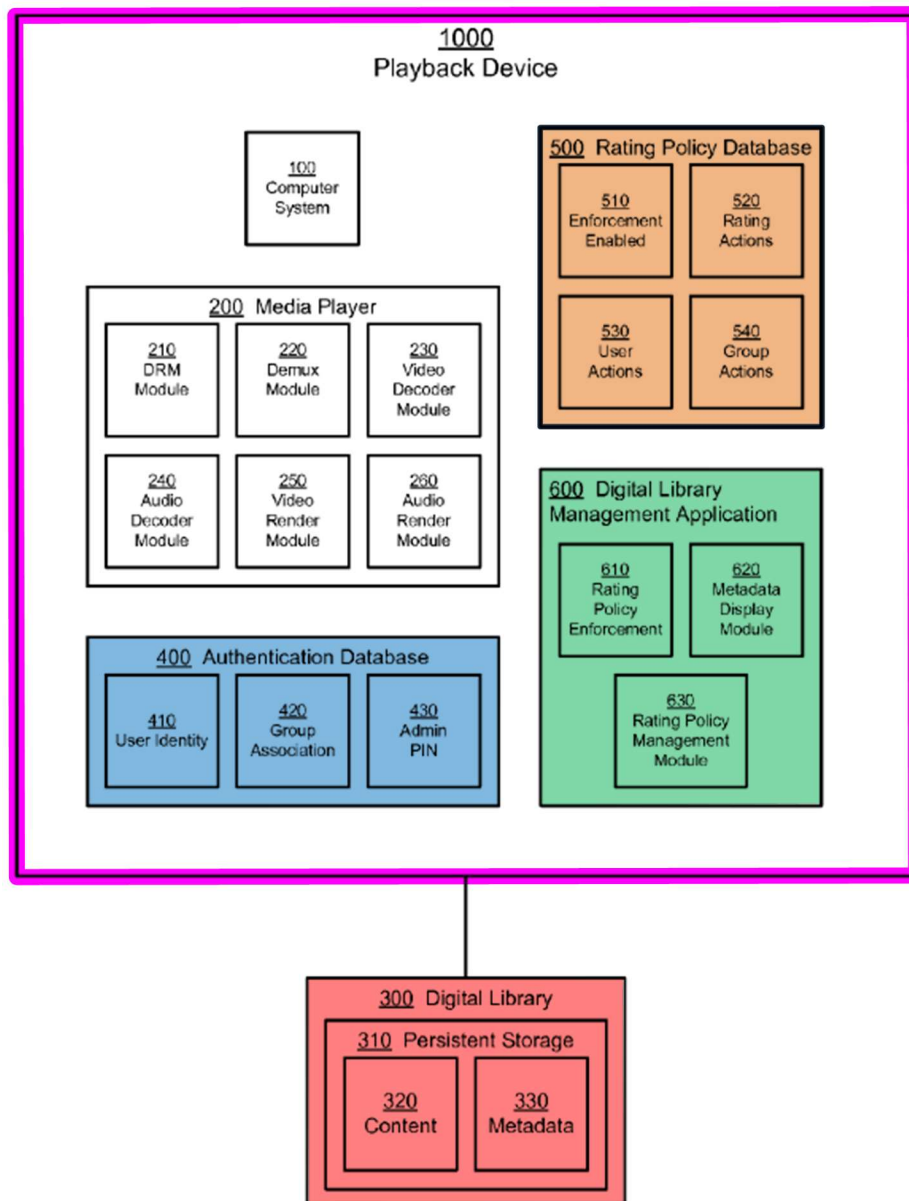


FIG. 2

Id., FIG. 2 (annotated).

The **digital library 300**, which stores content 320 and associated metadata 330, is coupled to or contained within **playback device 1000**. *Id.*, 5:6-10, 5:29-67. **Authentication database 400** includes user identity 410, which “contains user authenticators”; group associations 420, which “contain sets of users”; and administration PIN 430. *Id.*, 6:1-54. **Rating policy database 500** stores content rating override actions, which include actions that override a program’s original rating for identified users. *Id.*, 6:55-57, 7:3-21. **Digital library management application 600** includes a rating policy enforcement module 610 that “read[s] the V-chip policy for the appropriate content type and the content rating,” “determines if a rating action exists that overrides the V-chip blocking action based solely on the original content rating,” and uses **authentication database 400** and **rating policy database 500** “to determine if the user is able to watch the content.” *Id.*, 7:30-44, 8:58-9:10. **Digital library management application 600** also includes rating policy management module 630 that “allows the user to modify” data in **digital library 300**, **authentication database 400**, and **rating policy database 500**. *Id.*, 7:30-33, 7:55-58.

III. OVERVIEW OF PRIOR ART

A. Sullivan

Sullivan (Ex. 1005), filed June 24, 2004, and published February 3, 2005, is prior art under pre-AIA 35 U.S.C. § 102(a)-(b) and (e).

Sullivan discloses a content control system for limiting children's access "to certain types of content." Sullivan, Abstract. Sullivan recognizes that a user "may feel that a content rating for content the user has viewed may not be stringent enough, or conversely, too stringent, for sensitive users such as children, for whom access to the content is controlled by the user." Sullivan, [0006].

Sullivan provides "simplified control of parental lock settings." Sullivan, [0007]. The system includes a device interfaced to one or more audiovisual devices, each having "a native parental control subsystem or locking mechanism having adjustable parameters." Sullivan, [0009]. This system "allow[s] a user to input one or more general parental control parameters and then set[] the adjustable parameters to each native parental control subsystem within the system by mapping the parental control parameters onto each separate, native mechanism for each device." *Id.*

One such audiovisual device is "a content recorder" (e.g., a personal video recorder ("PVR")). Sullivan, [0095]. The content recorder includes "a hard disk drive" and "is used to receive and display television content." Sullivan, [0096]. The content recorder "prevent[s] unauthorized users from viewing restricted content" based on the rating of the content, a user's rating lock level, and an exception list. Sullivan, [0087]-[0089], [0095]-[0101].

Sullivan discloses a “parental locks interface” such as “content rating lock display screen 222” below. Sullivan, Abstract, [0002], [0037], [0039]. This screen allows a user to “select particular ratings to lock and unlock” and then press the “Turn On Parental Locks” button 244 “to turn on parental locks.” Sullivan, Abstract, [0039]-[0040], [0044], FIG. 4. A user’s selection of a particular rating locks that rating and all higher ratings. Sullivan, [0053].

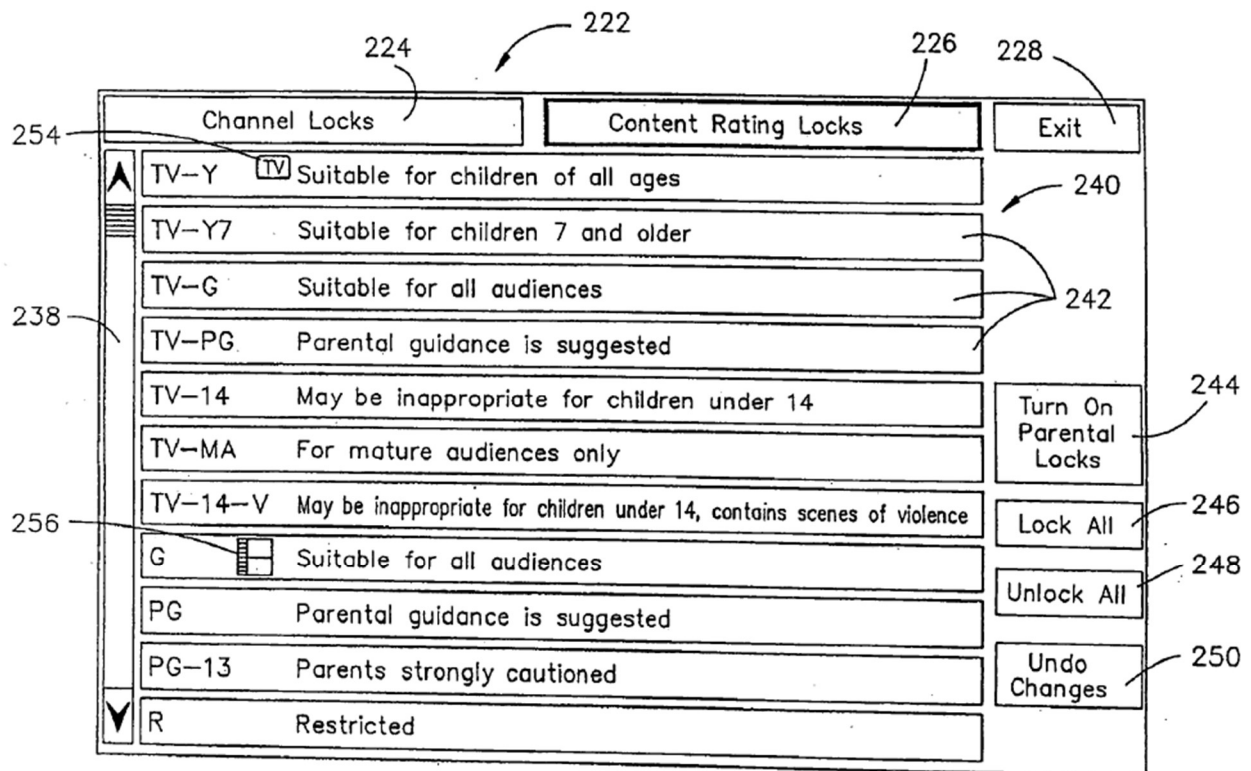


FIG. 4

Sullivan, FIG. 4.

“[S]eparate profiles could be selected for different children (or age groups),” with each profile assigned its own “individual acceptable content rating

parameters.” Sullivan, [0046]-[0047], [0051], [0088], [0092]. Sullivan discloses providing each user a “unique password” that, when entered, allows them to view ordinarily-blocked content stored on the PVR if a parent has added the user associated with that password to “an exception list” for that content. Sullivan, [0006]-[0007], [0074], [0077], [0089]-[0090], [0099]-[0100]. The process for adding a user to an exception list is depicted below.

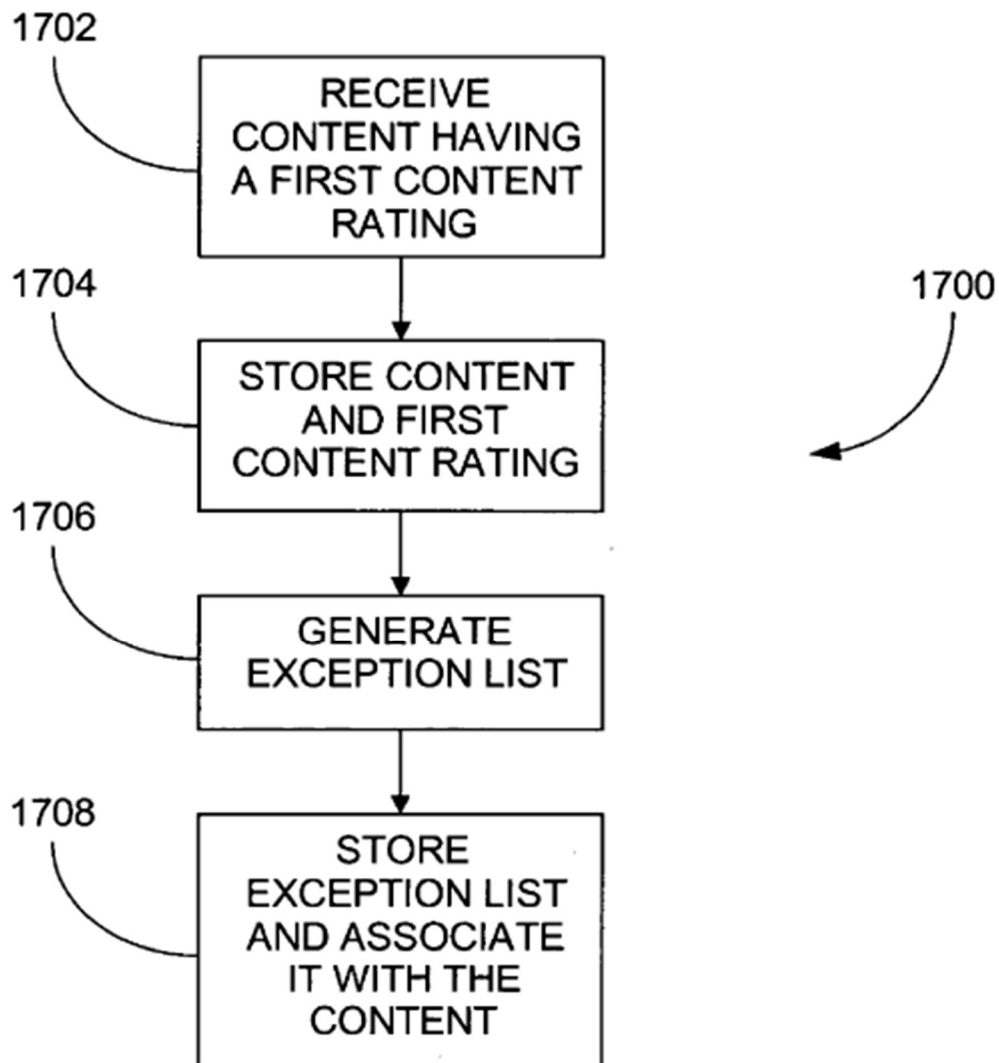


FIG. 17

Sullivan, FIG. 17.

B. Leung

Leung (Ex. 1006), filed October 16, 2001, and published July 18, 2002, is prior art under pre-AIA 35 U.S.C. § 102(a)-(b) and (e).

Leung discloses “exercising access control over television programs using a parental control user interface.” Leung, Abstract. The V-chip system allows “a consumer to program his or her television system to exclude programs” based on rating criteria. Leung, [0003]. Like the ’879 patent, Leung recognized that the V-chip’s effectiveness “depends on whether the consumer agrees with the subjective ratings,” contained in the vertical blanking interval (“VBI”) for each program. Leung, [0004]. Many users “will disagree with the rating systems and think that whatever exclusion programming they do will block out desirable programs while not blocking out undesirable programs.” Leung, [0005].

To address this, Leung provides “a combination of the V-Chip system and a parental control system more oriented around programming by a user for blocking and enabling particular television programs.” Leung, [0052]. Users can “override the operation of the V-Chip system for particular programs contained in user programmable enable override lists and blocking override lists.” *Id.* Figure 1, below, depicts “the operation of this override system.” Leung, [0053].

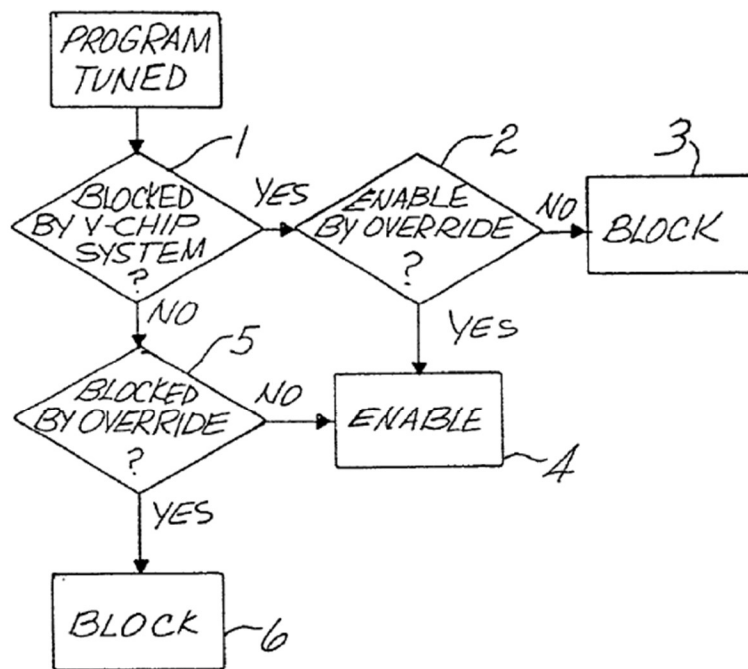


Fig. 1

Leung, FIG. 1.

The user-programmed rating criteria for excluding programs are stored and compared with the rating factor transmitted in the VBI. Leung, [0065]. Excluded programs are blocked unless they appear on “an enable override list.” *Id.*

Conversely, programs “not excluded under the rating criteria” are allowed unless they appear on “a blocking override list.” *Id.*

Leung discloses setting a “Master Password” to control the settings of the V-chip system and to “obtain access to all shows, areas of the guide[,] and features.” Leung, [0156]-[0157], [0181], [0183], [0203], FIG. 67. The password is a PIN entered “using the number keys on the remote.” Leung, [0181], FIG. 69. “If the

user does not input the Master Password, they will maintain access as defined by the User Profile.” Leung, [0156].

C. Craner

Craner (Ex. 1007), filed April 10, 2006, and issued December 13, 2011, is prior art under at least pre-AIA 35 U.S.C. § 102(e).

Craner discloses a parental control system implemented on user equipment “suitable for providing interactive media functionality,” including a PVR. Craner, 4:8-36, 4:60-5:10, 7:40-46. Figure 3, below, depicts a user interface “prompting a supervisor to create an administrative parental control access code, such as a personal identification number (‘PIN’), for accessing the content control application in privileged mode.” Craner, 9:3-7. “This parental control access code will be required for all subsequent administrative content control access requests.” Craner, 9:11-13, 9:66-10:11, FIG. 4.

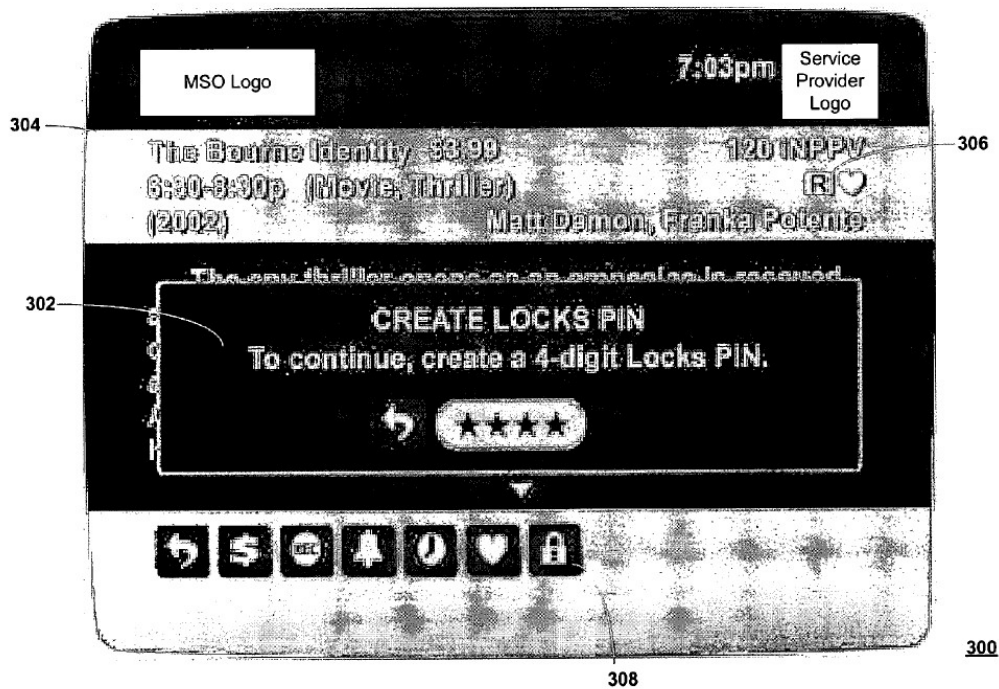


FIG. 3

Craner, FIG. 3.

The supervisor may create “customize[d] parental control settings” for multiple users, each of whom “may be authenticated upon accessing or powering on the user equipment [(or “at other convenient times”)] using a standard username and password combination, a verification module (e.g., voice, iris, or fingerprint verification), or any other convenient method.” Craner, 11:48-59, 12:7-43.

Figure 6, below, depicts a “locks setup display screen 600” for one user. Craner, 11:48-50.

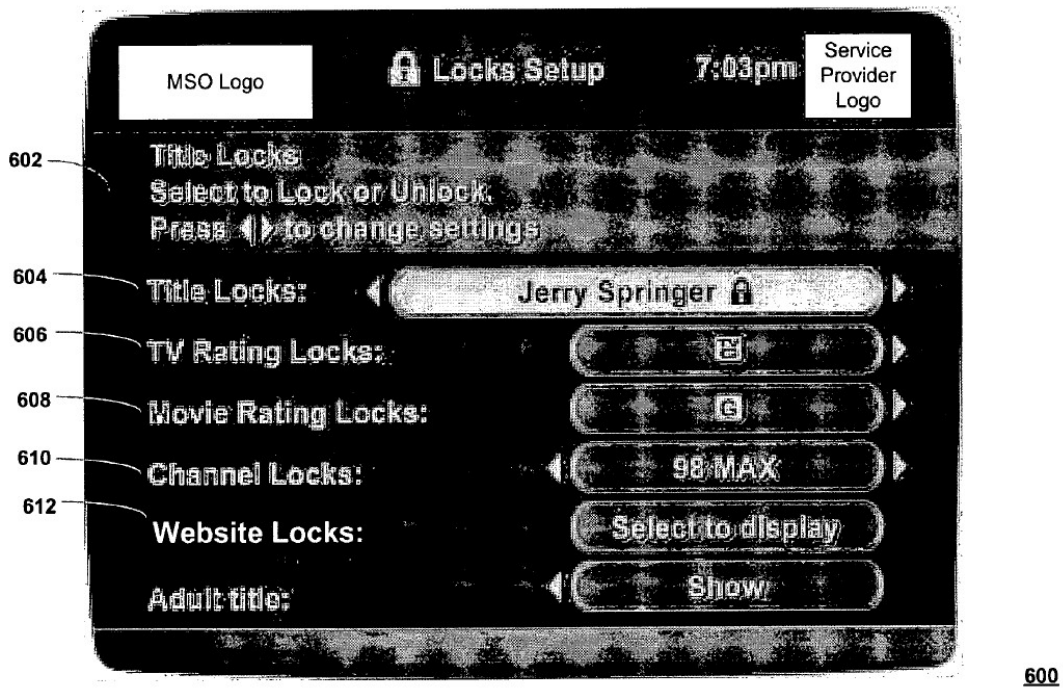


FIG. 6

Craner, FIG. 6.

Craner discloses that “parental control access codes may also be given to users (e.g., children) of the system in order to access media and other assets.” Craner, 10:28-30. If the “user attempts to access media content not permitted by the user’s parental controls,” the user may enter the access code, when prompted, to access the selected asset (e.g., a “recorded program that the user would be otherwise incapable of accessing (due to parental control locks).” Craner, 10:30-43, 10:51-55.

Figure 15, below, illustrates a process for determining whether the requested asset is blocked and, if so, whether the user is entitled to access the asset. Craner, 20:24-21:20.

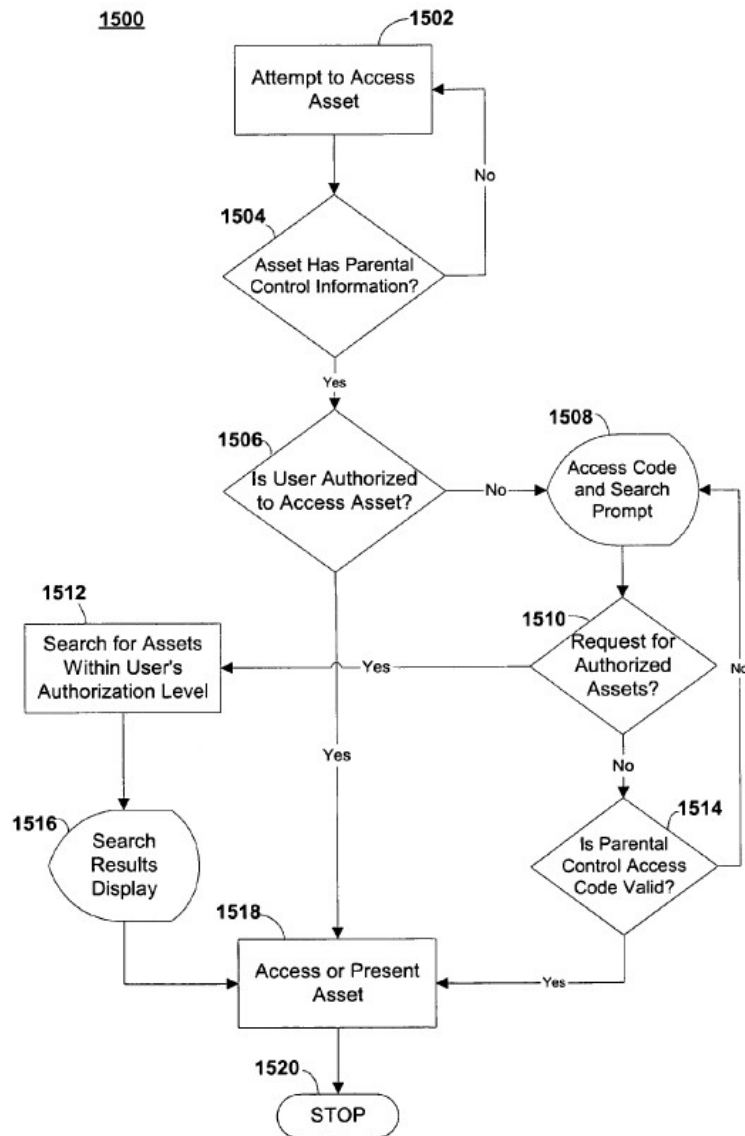


FIG. 15

Craner, FIG. 15.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) would have had a bachelor’s degree or equivalent in electrical engineering, computer science, or a related field, in addition to two years in research, design, or development in television broadcast or video playback systems or other comparable experience. Houh ¶20.

V. CLAIM CONSTRUCTION

No terms need to be construed to resolve the unpatentability issues in this Petition. *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).¹

VI. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Claims 1-19 Are Obvious over Sullivan, Leung, and Craner

1. Rationale for Combining Sullivan and Leung

A POSITA would have found it obvious to combine Sullivan and Leung to implement a playback device having a V-chip and an apparatus that enforces

¹ Petitioner reserves the right to argue that certain limitations in the challenged claims are indefinite and/or require construction to resolve other controversies in other forums.

rating-based access controls for digital content in a digital library on a per media and per user basis.

a. Combining Sullivan and Leung to implement a V-chip on Sullivan's PVR

Sullivan's content recorders (e.g., PVRs) allow users to access "ratings enabled media" like "broadcast television" and "video on demand services" and store content and its associated rating for subsequent playback. Sullivan, [0012], [0033], [0063], [0095]-[0096], [0099]. Sullivan discloses a user interface providing "a single point of user control for parental locks for multiple audio and/or audiovisual devices" within an entertainment system, each having a "native parental control subsystem." Sullivan, Abstract, [0002], [0009]. The user interface (e.g., below) allows a parent to set acceptable content rating parameters by selecting "a particular rating" from [rating cells 242](#) and locking "that rating and all higher ratings." Sullivan, [0039], [0053], [0063]-[0064]. The interface includes a [button 244](#) that "turn[s] on parental locks after a user's selections have been made by mapping a user's selections to each native parental control subsystem." Sullivan, [0009], [0040], FIG. 4.

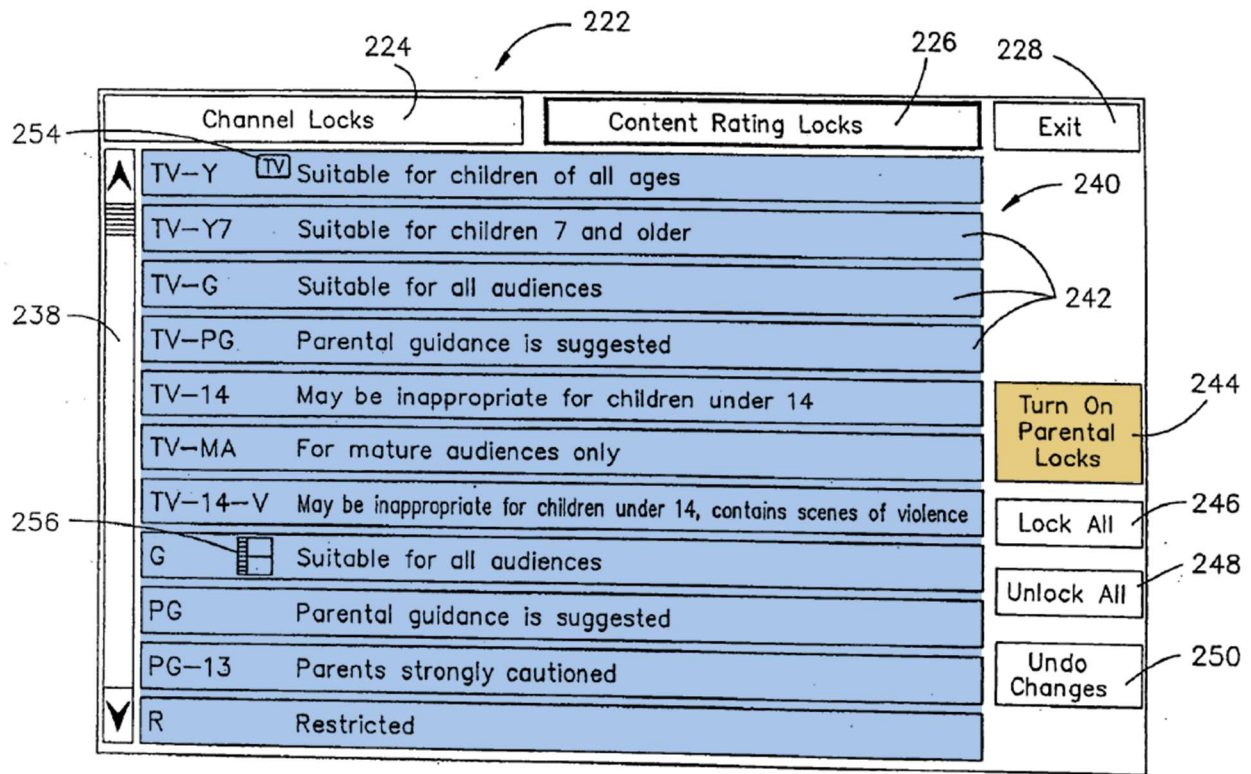
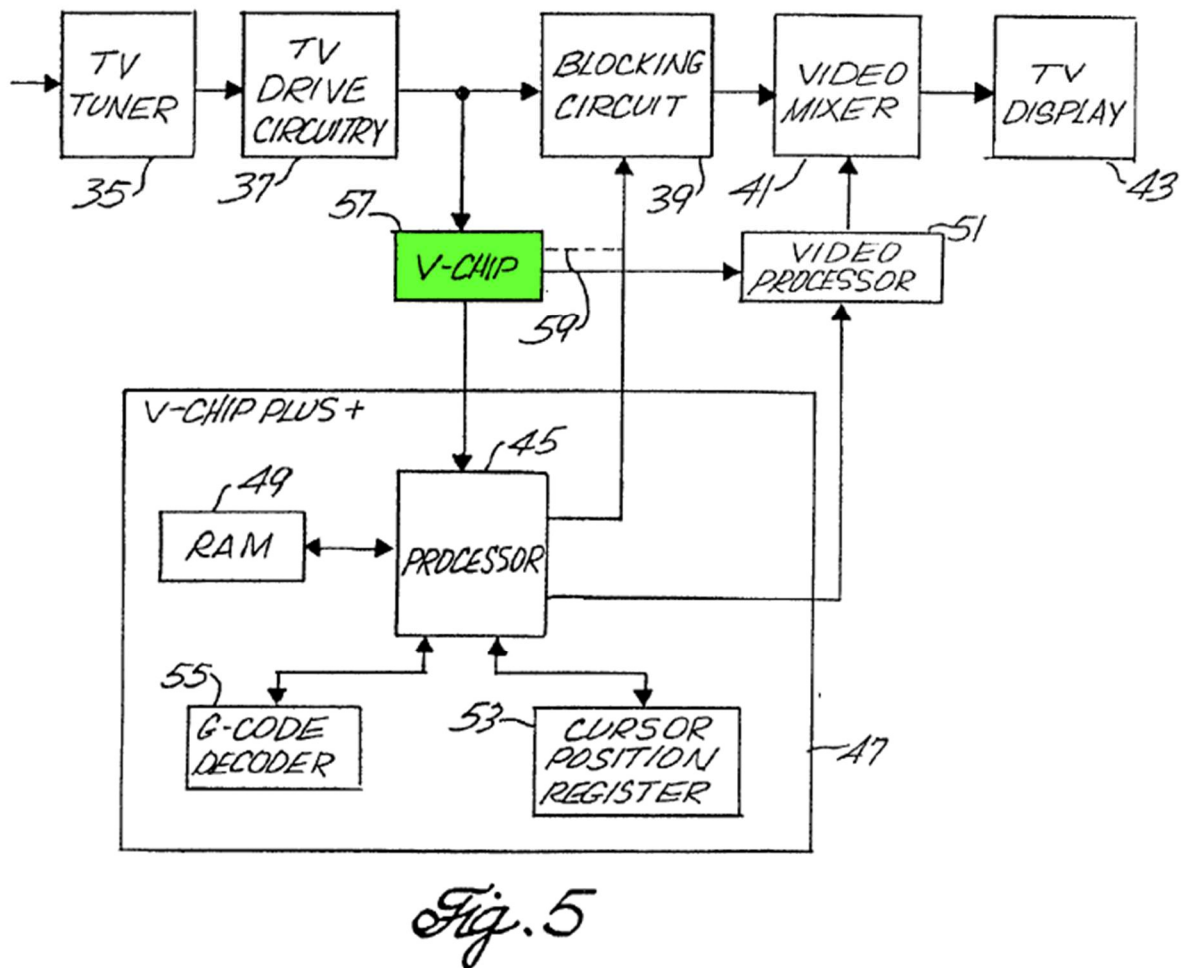


FIG. 4

Sullivan, FIG. 4 (annotated).

A POSITA would have found it obvious from Leung to implement Sullivan's ratings-based parental locks on Sullivan's PVR using Leung's V-chip within the PVR's native parental control subsystem. Houh ¶66. A V-chip, highlighted below, allows parents to program their "television system to exclude programs according to their preferred" rating levels and generates a blocking signal if the program rating violates the programmed rating levels. Leung, [0003], [0078], [0082]-[0088].



Leung, FIG. 5 (annotated).

A POSITA would have been motivated to use Leung's V-chip to implement Sullivan's ratings-based parental locks because doing so would have involved combining prior art elements according to known methods to predictably yield a user-friendly parental control subsystem for performing Sullivan's ratings-based parental lock. Houh ¶67. Sullivan recognizes that "many televisions now include devices that decode program rating data encoded into a program at the time it is broadcast to selectively pass or block television programming based on the rating

level set.” Sullivan, [0003]. The V-chip was one well-known such device.

Sullivan ’365, 1:18-22; Houh ¶67. Indeed, V-chips have been mandated in *all* U.S. televisions since 2000. Ex. 1001, 1:19-22.

A POSITA would have recognized that Sullivan’s PVR implements functionality commonly performed by a V-chip. Houh, ¶68; Sullivan, [0053], [0096]-[0101]. Sullivan teaches a PVR receiving and storing a television signal with the program rating included in the VBI and preventing access to restricted content based on the program rating and the acceptable content rating parameters. *Id.* V-chips were designed to extract the program rating from the VBI and generate a blocking signal if the rating exceeded the acceptable content rating parameters. Leung, [0003], [0065], [0078], [0084]. A POSITA would have been motivated to incorporate Leung’s V-chip in Sullivan’s PVR because many consumers would have been familiar with the V-chip’s use and operation, and because V-chips were well known to perform the desired functionality, including extracting a program rating from the VBI and preventing access to restricted content. Sullivan, [0095], [0098], [0101]; Leung, [0003], [0065], [0078], [0084]; Houh ¶68.

A POSITA would have reasonably expected success in implementing Leung’s V-chip in Sullivan’s television. Houh ¶69. Sullivan discloses that the television content includes a rating in the VBI, and V-chips are designed to use the VBI to identify the program’s rating. Sullivan, [0098]; Leung, [0003], [0065],

[0078], [0084]. Accordingly, implementing Leung's V-chip in Sullivan's PVR would have required simply applying conventional techniques to use the V-chip for its intended purpose. Houh ¶¶69. Moreover, Leung teaches how to override the V-chip's blocking signal, teaching a POSITA how to implement Sullivan's similar features that override the default ratings-based parental locks. *Id.*

b. Combining Sullivan and Leung to implement access controls for digital content in a digital library on a per media and per user basis that overrides the default V-chip policy

A POSITA would also have found it obvious from Leung to implement access controls for digital content in Sullivan's PVR's digital library on a per media and per user basis that overrides the PVR's default V-chip policy. Houh, ¶¶70-77.

As Figure 13 shows, Sullivan discloses that if "a user requests content" via the user interface, "[t]he content control system, upon receiving the user request, determines if the example content is blocked ... , for instance, because its content rating exceeds the rating threshold delineated by previously set acceptable content rating parameters of the content control system." Sullivan, [0072]-[0073], FIG. 13. If blocked, the user must enter an access code/password to access the content. Sullivan, [0074]. "[U]nauthorized viewers, such as children, who do not possess the necessary password" cannot access the content. *Id.*

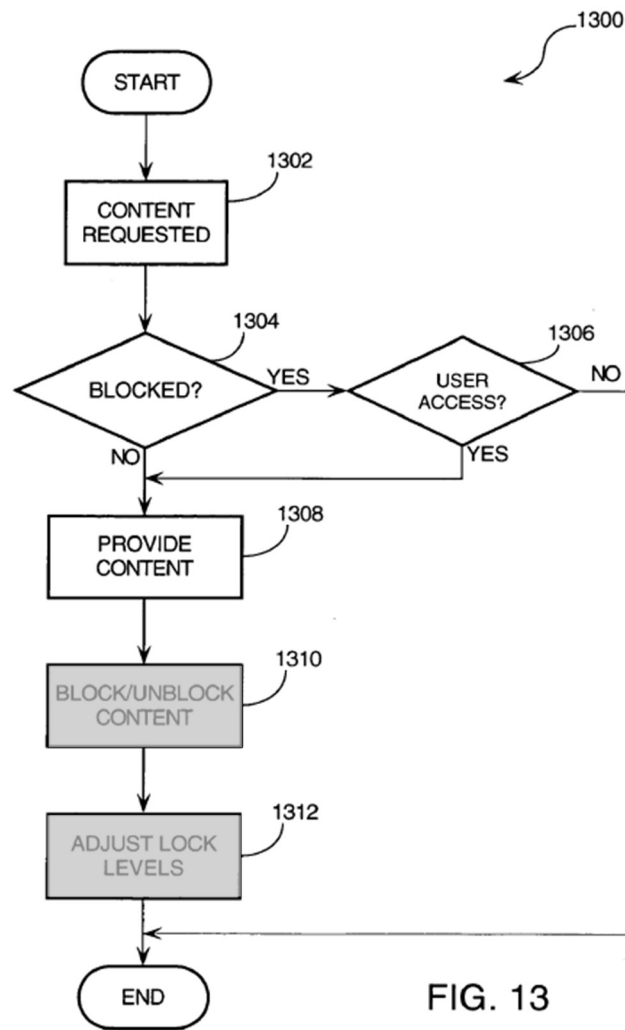


FIG. 13

Sullivan, FIG. 13 (annotated).

Sullivan also discloses that a PVR “may include a unique password” for each PVR user (e.g., a seven-year-old child and a thirteen-year-old child may have different passwords). Sullivan, [0099]. A parent may generate an “exception list associated with” “a specific instance of audio/visual content,” where the list identifies “at least one user who is allowed to access the content and who would otherwise be blocked by application of the content rating.” Sullivan, [0099]-

[0100]. The PVR then “prevent[s] unauthorized users from viewing restricted content.” Sullivan, [0101].

A POSITA would have been motivated to combine Sullivan and Leung to override the V-chip’s default ratings-based parental locks on Sullivan’s PVR if the PVR authenticates the password of a user included on an exception list associated with the requested content. Sullivan’s system allows “authorized users” to access otherwise blocked content if they input their access code/password. Houh, ¶73. Sullivan, [0072]-[0074], [0077]. Because Sullivan teaches providing each PVR user a “unique” access code/password and creating exception lists identifying users that are allowed to view specific content, a POSITA would have understood that Sullivan’s system would have treated any of the users identified on an exception list as “authorized” to view the associated content and allowed access to the requested content upon authenticating any of the access codes/passwords associated with the users identified on the associated exception list. Houh, ¶73; Sullivan, [0099]-[0101]. A POSITA would have been motivated to do so to allow parents granular control over the content that multiple users of different ages and maturities may access, including allowing particular users to access recorded content whose rating the parent deems too stringent for those users without modifying the V-chip rating policy. Houh ¶73; Sullivan, [0006], [0088]-[0089], [0099]-[0101].

A POSITA would have seen this process of overriding Sullivan’s default ratings block enforced using Leung’s V-chip upon authenticating a password associated with a user identified on an exception list as combining familiar elements according to known methods to yield predictable results because Leung discloses a similar process for overriding its default V-chip policy. Houh ¶74. Leung discloses that “[w]hen a show is blocked,” for example, based on its rating, “and a user without entering the Master Password tries to access a blocked element, access to the blocked element will be denied and a dialog box requesting the Master Password will be displayed (see FIG. 66),” depicted below. Leung, [0156]-[0157], [0186]. Failure to correctly input the password “will result in maintaining the block,” but “[u]pon entering a correct password, the program is unblocked.” Leung, Abstract, [0156]-[0157], [0186]-[0192]. While Leung’s system lacks multiple user profiles, each with its own password for individualized parental controls, a POSITA would have been motivated to maintain Leung’s familiar user experience of using passwords to override a V-chip blocking policy in Sullivan’s system with multiple users having their own unique access code/password to allow access to content based on their particular profile. Sullivan, [0089], [0099]; Houh ¶74.

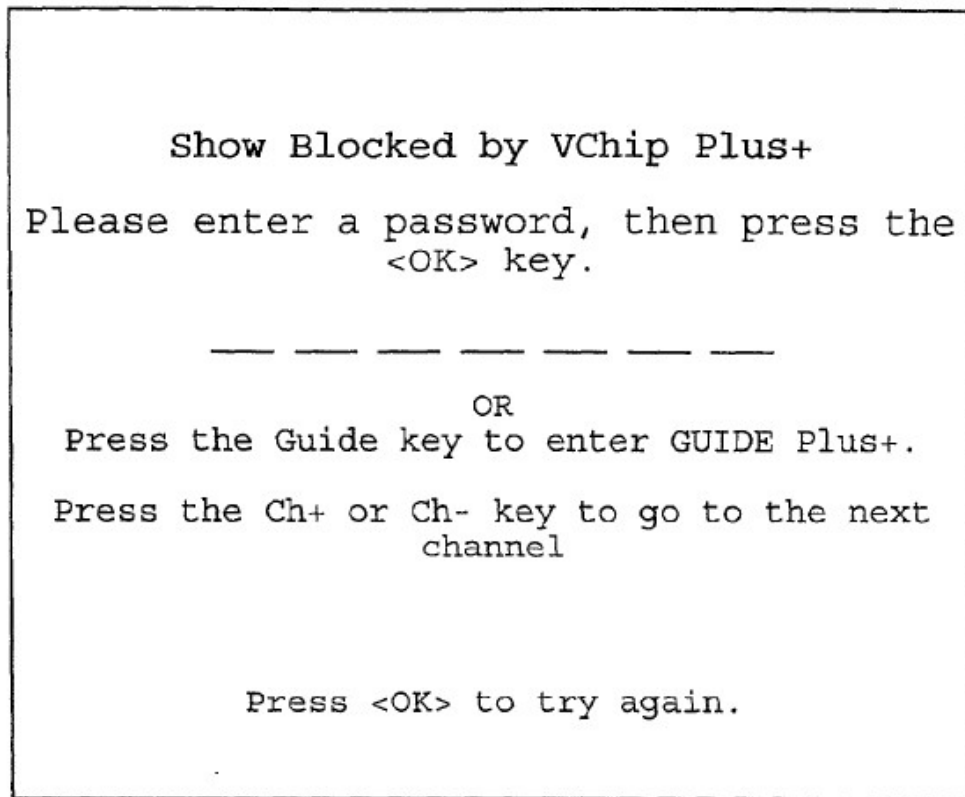


FIG. 66

Leung, FIG. 66.

A POSITA would have reasonably expected success in the combination because it would have required implementing only conventional techniques for determining whether an entered access code/password matches an access code/password associated with a user identified on the requested content's exception list and, if so, overriding a blocking signal. Houh ¶75. Indeed, Sullivan already discloses each user entering "his or her user identification via the user interface to access content via the information appliance," and Leung teaches how to use its V-chip in combination with other criteria (e.g., override lists) to override

a V-chip's blocking signal, giving a POSITA a reasonable expectation of success in implementing Leung's V-chip with Sullivan's exception lists. Sullivan, [0089]-[0090]; Leung, [0082]-[0090]. Moreover, storing multiple access codes/passwords that may provide access to blocked content was already well known. Houh ¶75. Craner, *e.g.*, taught user equipment (e.g., a PVR) determining whether "the user has entered a valid parental control access code" to access blocked content by comparing the inputted code "to a list of authorized parental control access codes stored on the user equipment" and granting access "[i]f the access code is valid." Craner, 20:24-21:20, FIG. 15.

If Patent Owner argues Sullivan's exception lists are not rating based access controls, a POSITA would have further been motivated to modify Sullivan's exception lists by allowing parents to identify users *and* a rating associated with the content for each identified user because doing so would have improved Sullivan's system by allowing parents to both allow users to access content who would otherwise be blocked from doing so *and* to block users from accessing the same content who would otherwise be allowed to do so. Houh ¶76; Sullivan, [0006], [0095]-[0100]. Sullivan suggests such a modification to its exception lists because it recognizes that parents may view the original content rating as either too stringent or not stringent enough and discloses "a need for a content control system that allows a user to modify the content rating of media recorded by a content

recorder as the user sees fit.” Sullivan, [0006]-[0007], [0095]-[0096]. For example, Sullivan discloses an embodiment where a parent changes the rating of a TV-14 program to either TV-PG or TV-MA. Sullivan, [0095]-[0096]. Because Sullivan teaches that it “may be undesirable” to permanently alter the rating stored with the associated content, a POSITA would have recognized this modification to the exception lists as beneficial. It would have allowed a parent to specify a rating to apply for each child when the parent disagrees with the original rating without permanently overwriting the stored rating. Houh ¶76; Sullivan, [0006], [0099].

A POSITA would have additionally found this modification obvious, would have been motivated to make it, and would have reasonably expected success in view of Leung’s override lists. Leung, for example, discloses applying the V-chip’s default rating policy and then checking an “enable override list” or a “blocking override list” to determine if a parent has chosen to override the V-chip’s default rating policy for the selected program. Houh ¶77; Leung, [0052]-[0057]. Leung also discloses that these lists may be “combined into a single list.” Leung, [0097]. If, after checking the list, the system determines that the program is blocked, it requires inputting a password to view the program. Leung, Abstract, [0088]. Because Leung discloses a list that identifies both programs to block and programs to allow, and because Sullivan discloses an exception list identifying users and the ability to change a program’s rating, a POSITA would have seen

modifying Sullivan’s exception list as combining familiar elements (e.g., setting a rating that differs from the original rating and using an exception list to control which users may access the requested content without modifying the default V-chip rating policy when the parent disagrees with the original rating) to achieve a predictable result—a content control system that determines whether the requested content is blocked based on its rating (either its original rating or the rating(s) specified on an exception list) and requiring a password to view the content if it is blocked. Houh ¶77; Sullivan, [0072]-[0074], [0077], [0099]-[0100]; Leung, [0082]-[0090].

2. Independent Claim 1

- a. **[1pre]: “An apparatus for setting rating based access controls for known digital content to be played on a video playback device having a V-chip, the apparatus comprising:”**

If limiting, Sullivan and Leung teach [1pre]. Houh ¶¶78-81.

Sullivan’s PVR (video playback device) stores “television content” and allows playback of stored content on a “content viewing device.” Sullivan, [0034], [0093], [0095]-[0101]. As discussed in Section VI.A.1.a, it would have been obvious to implement Sullivan’s PVR using a V-chip, as taught by Leung. Houh ¶79.

Sullivan's PVR, which includes the native parental control subsystem, is "[a]n apparatus." Sullivan, Abstract, [0009], [0012]; Houh ¶80. This apparatus allows "setting rating based access controls for known content to be played" by the PVR because, if an authorized user (e.g., parent) "feel[s] that a content rating for content the user has viewed" is "too stringent" for particular users, the apparatus allows setting an exception list identifying users "allowed to access the content and who would otherwise be blocked by application of the content rating." Sullivan, [0006]-[0007], [0046]-[0050], [0088]-[0089], [0099]-[0100]. Additionally, as discussed in Section VI.A.1.b, it would have been obvious to modify Sullivan's exception lists to identify both a user and a corresponding rating for the associated content. Houh ¶80. Based on the stored content's rating, the acceptable content rating parameters of the V-chip (implemented in Sullivan's PVR based on Leung, see Section VI.A.1.a), and an exception list associated with the content, the apparatus allows authorized users to play the requested content. Sullivan, [0074], [0077], [0089], [0095]-[0101]; *supra* Section VI.A.1.

The PVR's stored content is "known digital content" because the PVR records the content as compressed or uncompressed data on "a hard disk drive," which was a well-known type of digital storage medium. Sullivan, [0096]-[0100] (using MPEG-2 compression); Walls, [0003] (a PVR's hard disk "digitally records live television (TV) programs" for playback); Baumgartner, [0062] (a "hard disk

drive” is “a digital storage device”); Houh ¶81. The PVR’s content is “to be played on a video playback device having a V-chip” because Sullivan’s PVR (implemented with Leung’s V-chip, see Section VI.A.1.a) “is used to receive and display [the] content.” Sullivan, [0096]; *see also id.*, [0032].

b. [1a]: “a rating policy management module for selectively setting rating based access control on a per media and per user basis for digital content of a digital library thereby overriding a policy set by the V-chip for access to the digital content from the video playback device; and”

Sullivan and Leung teach [1a]. Houh ¶¶82-86.

Sullivan teaches “a rating policy management module for selectively setting rating based access control... for digital content of a digital library.” Houh ¶83. Sullivan’s PVR is a “hardware system” “controlled by a central processing system 102,” including “a central processing unit” that executes stored instructions that implement Sullivan’s content control system. Sullivan, [0012], [0031], [0033], [0094]. These instructions, for example, allow adding recorded content and an associated rating to the PVR’s hard disk drive, creating a profile and “unique password” for each user or group of users, and creating exception lists. Sullivan, [0046]-[0050], [0088]-[0090], [0095]-[0101]; *supra* Section VI.A.1.b. A POSITA would have understood that the instructions that execute this functionality and the other functionality of the content control system discussed in this section constitute

the rating policy management module. Houh ¶83. This aligns with the '879 patent's disclosure of a "rating policy management module." Ex. 1001, 7:55-58, 11:1-37; Houh ¶83. At a minimum, such a module would have been obvious, as modules were well-known ways to organize functionality for software programs. Houh ¶83.

Sullivan's PVR permits control of "digital content of a digital library" because the PVR includes a hard disk drive digitally storing television content for later viewing. Sullivan, [0095]-[0101]; Houh ¶84; *supra* [1pre]. Sullivan teaches that the PVR may "provide controls for selecting a particular media to access" from "multiple media" on the PVR. Sullivan, [0067], [0095]-[0101]; Houh ¶84.

As discussed in Section VI.A.1.b, Sullivan and Leung teach "selectively setting rating based access control on a per media and per user basis for digital content of a digital library thereby overriding a policy set by the V-chip for access to the digital content from the video playback device." Houh ¶85. For example, the content control system allows a parent to create exception lists maintained on the PVR. Sullivan, [0099]-[0100]. Each exception list is associated with "a specific instance of audio/visual content" ("per media basis") on the PVR and identifies users ("per user basis") allowed to access this content who would otherwise be blocked based on application of its content rating ("overriding a policy set by the V-chip for access to the digital content from the video playback device"). *Id.*;

supra Section VI.A.1.b. Additionally, as discussed in Section VI.A.1.b, it would have been obvious to modify Sullivan’s exception lists to identify both a user and a content rating and to apply this content rating when the corresponding user attempts to access the content. Houh ¶85.

- c. **[1b]: “a rating policy enforcement module for enforcing rating based access to the individual digital content for a plurality of users separate from and in addition to an administrator,”**

Sullivan teaches [1b]. Houh ¶¶86-89.

For the reasons discussed for [1a], a POSITA would have understood that the instructions that execute the functionality of the content control system discussed in this section constitute the “rating policy enforcement module for enforcing rating based access.” Houh ¶87. These instructions determine whether requested content is blocked and, if so, override the default V-chip policy if the user enters a password corresponding to a user allowed to access the content based on the policy specified by the associated exception list. *Supra* Section VI.A.1.b; Houh ¶87. This aligns with the ’879 patent’s disclosure of a “rating policy enforcement module.” Ex. 1001, 7:34-40; Houh ¶87. At a minimum, such a module would have been obvious, as modules are well-known ways to organize functionality for software programs. Houh ¶87.

Sullivan's PVR enforces access "for a plurality of users separate from and in addition to an administrator" because Sullivan discloses that an "authorized user, such as a parent," is an administrator that may create profiles for a plurality of users, including a seven-year-old child and a thirteen-year-old child, where each profile includes "a unique password." Houh ¶88; Sullivan, [0088]-[0089], [0099]. The administrator must "enter a password to prevent tampering with the parental control system by members of the protected audience." Sullivan, [0087].

Sullivan's PVR enforces rating based access "to the individual digital content" because access is to "a specific instance of audio/visual content" on the PVR for the users. Sullivan, [0099]-[0100]; *supra* Section VI.A.1.b; Houh ¶89. The PVR's content control system determines if the requested content is blocked "because its content rating exceeds the rating threshold delineated by previously set acceptable content rating parameters of the content control system." Sullivan, [0072]-[0073]. If so, the system allows access when the user enters an access code/password that corresponds to a user who appears on the associated exception list. Sullivan, [0074], [0077], [0089]-[0090], [0099]-[0100]; *supra* Section VI.A.1.b; Houh ¶89.

- d. **[1c]: "wherein at least a first user and a second user of the plurality of users have different media rating requirements and**

**have different media ratings associated
with a same specific digital content,”**

Sullivan and Leung teach [1c]. Houh ¶¶90-93.

Sullivan discloses that first and second users of the plurality of users have different media rating requirements. Houh ¶91. Sullivan discloses creating “multiple user profiles ... for individual users or groups of users,” where each profile has “individual acceptable content rating parameters set specifically for that user or group of users.” Sullivan, [0088]. Sullivan discloses that “a young child” (e.g., the seven-year-old child) (second user) “may have more restrictive acceptable content rating parameters than would a teen-aged child” (e.g., the thirteen-year-old child) (first user). Sullivan, [0088], [0099].

Sullivan teaches that the first and second users have different media ratings associated with a same specific digital content. Houh ¶92. Sullivan discloses that a thirteen-year-old user “may be allowed to access a previously recorded television program rated TV-14” when a parent adds that user to an exception list. Sullivan, [0099]-[0100]. A POSITA would have understood that this teaches different media ratings associated with a same specific digital content because the seven-year-old user, who has “one password” and does not appear on the associated exception list, cannot access the program based on its TV-14 rating, whereas the thirteen-year-old user, who has “another password” and appears on the exception list, can access the

program upon entering the associated password. Sullivan, [0006], [0088]-[0089], [0099]-[0100]; *supra* Section VI.A.1.b; Houh ¶92.

Moreover, as discussed in Section VI.A.1.b, Sullivan and Leung additionally render obvious modifying the exception list associated with the requested content to allow a parent to specify different media ratings for each user if the parent disagrees with the original media rating as it pertains to each user. Sullivan, [0006]-[0007], [0095]-[0100]; Leung, [0052]-[0055]. This would have been beneficial so that a change to the default ratings-based policy enforced by the V-chip would not impact a parent's decisions regarding whether to grant or deny each child access to particular content. Sullivan, [0045]; *supra* Section VI.A.1.b; Houh ¶93.

- e. **[1d]: “wherein a first of the two users is allowed to access the specific digital content based upon a first authentication code and a second of the two users is blocked from access to the specific digital content based upon a second authentication code,”**

Sullivan teaches [1d]. Houh ¶¶94-95.

Sullivan discloses that each user or group is provided “a unique password” to access content on the PVR. Houh ¶95; Sullivan, [0099]. Sullivan discloses that a seven-year-old child (a second of the two users) “may have one password,” and a thirteen-year-old child (a first of the two users) “may have another password.” *Id.*

If the first user appears on an exception list for a television program rated TV-14, the user's password (first authentication code) allows them to access the associated specific digital content. Sullivan, [0074], [0089]-[0090], [0099]-[0101]. If the second user, who has "more restrictive acceptable content rating parameters" than the first user, does not appear on the exception list for this program and enters their password (second authentication code), the PVR will block access to the restricted content based on comparing the original content rating and the active ratings policy for the PVR. Sullivan, [0074], [0088], [0099]-[0101].

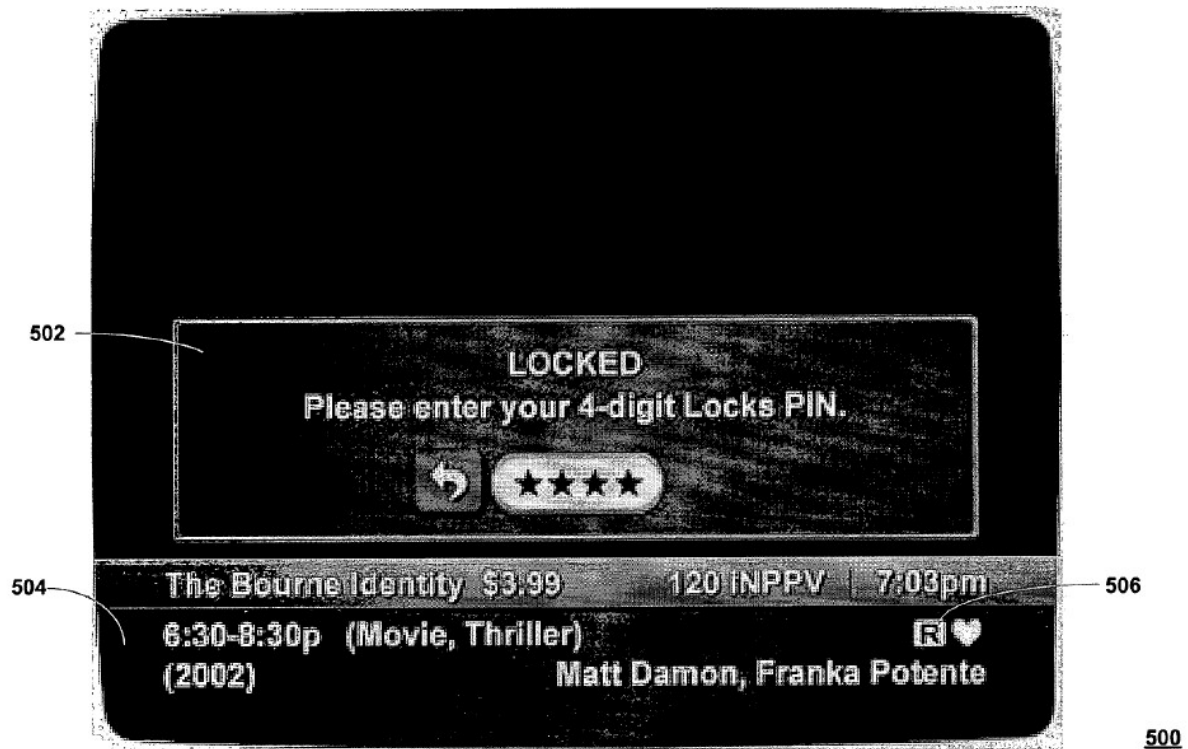
f. [1e]: "wherein the first authentication code comprises a personal identification number (PIN),"

Sullivan or Sullivan and Craner teach [1e]. Houh ¶¶96-100.

As discussed for [1d], the first user's password is a "first authentication code." Sullivan, [0099]; Houh ¶97. Sullivan also refers to a user being provided an associated "access code, password[,] or the like," or a "personal identification code," which a POSITA would have recognized encompasses a "PIN." Houh ¶97; Sullivan, [0074], [0077]-[0078], claim 19.

If Patent Owner argues Sullivan does not teach a "PIN," a POSITA would have found it obvious from Craner to implement Sullivan's password/access code for each user as a PIN. Houh ¶98. PINs were widely used to grant access, including to restricted television content. *See, e.g.,* Leung, Abstract, [0181], FIG. 69;

Novack, [0007]. Craner discloses using PINs for users “to access media and other assets,” as illustrated below. Craner, 9:3-7, 10:28-46, 11:36-43, 21:8-20; FIGS. 3-5; Houh ¶98.



Craner, FIG. 5.

A POSITA would have been motivated to use Craner’s PINs as Sullivan’s passwords/access codes to facilitate the user’s entry using a “remote control device” like Sullivan’s, which commonly included a numerical keypad and lacked letter keys. Sullivan, [0069]; Leung, [0090], FIG. 6; Houh ¶99; *see* Jarman, [0036]. A PIN would also have been faster for users and simpler for children, whom Sullivan envisions as users. Houh ¶99. Implementing Sullivan’s password/access

code as a PIN would have simply combined prior art elements according to known methods to predictably yield an authentication code that is easy for users to enter into the system, thereby saving users time. Houh ¶¶99.

A POSITA would have reasonably expected success implementing Sullivan’s password/access code as a PIN, as this would have simply combined prior art elements according to known methods to yield the predictable result of authentication using a PIN—something the ’879 patent recognizes that prior art systems did. Houh ¶¶100; Ex. 1001, 1:60-63, 2:44-48.

g. [1f]: “wherein the different ratings associated with the specific digital content are enforced using the first and second authentication codes, and”

Sullivan or Sullivan and Leung teach [1f]. Houh ¶¶101-102.

Sullivan discloses that the television program (“specific digital content”) and its rating are “saved by the PVR on a hard disk drive.” Sullivan, [0096]-[0100]. If a user selects the program and it is blocked, the user enters their password. Sullivan, [0072]-[0074], [0089]-[0090], [0099]. The thirteen-year-old’s password corresponds to the “first authentication code,” and the seven-year-old’s password corresponds to the “second authentication code.” *Supra* [1d]. The “different ratings associated with the specific digital content” (*supra* [1c]) are enforced using these “first and second authentication codes” because Sullivan’s content control system

only allows access to the content if the user appears on the exception list and the password/access code entered by the user is authenticated. Sullivan, [0073]-[0074], [0089]-[0090], [0099]-[0100]; *supra* Section VI.A.1.b; Houh ¶102. For example, the content control system enforces the rating for the thirteen-year-old associated with a content rated TV-14 because once it determines that the thirteen-year-old's user identifier appears on the exception list for the content, it authenticates the first authentication code to allow access by the thirteen-year-old to the content. And the content control system enforces the rating for the seven-year-old associated with the content rated TV-14 because the second authentication code cannot be used to access the content. Sullivan, [0099]-[0100]; Houh ¶102. Alternatively, where Sullivan's exception lists are modified based on Leung to allow parents to specify different ratings for each user on one exception list, *supra* Section VI.A.1.b, Sullivan's content control system would similarly use the first and second authentication codes to determine which media rating to apply because the entered authentication code would identify the user, causing the content control system to determine the rating associated with that user. Houh ¶102.

- h. [1g]: “wherein the first of the two users is allowed to access the specific digital content in response to determining that a content identifier of the specific digital content matches a user identifier of the first user and the personal identification**

**number of the first user is successfully
authenticated.”**

Sullivan and Leung teach [1g]. Houh ¶¶103-105.

A POSITA would have understood Sullivan and Leung to teach or at least render obvious “determining that a content identifier of the specific digital content matches a user identifier of the first user.” Houh ¶104. Sullivan’s exception lists (implemented according to Leung, *supra* Section VI.A.1.b) associate each “instance of audio/visual content stored by the PVR” (“the specific digital content”) with a user (“the first user”) that is allowed to watch the audio/visual content (even though, based on the content’s rating, the user would not be).

Sullivan, [0099]-[0100], Figure 17. A POSITA would have recognized that, to reflect these associations, Sullivan’s exception lists would associate an indication of the audio/visual content (“a content identifier of the specific digital content”) with an indication of the user (“a user identifier of the first user”). Houh ¶104. For example, Sullivan’s exceptions lists may indicate that a particular user is allowed to watch a particular television show by including an indication of the user and an indication of the television show. To determine whether the user is allowed to watch the television show, Sullivan’s PVR uses the exception lists to determine whether the indication of the television show (“a content identifier of the specific digital content”) is associated on an exception list (“matches”) with the indication

of the user (“a user identifier of the first user”) and, if so, requests the user provide the appropriate access code/password. Sullivan, [0067], [0072], [0099]-[0100]; Houh ¶104.

Sullivan teaches that “the first of the two users is allowed to access the specific digital content in response to determining that a content identifier of the specific digital content matches a user identifier of the first user and the personal identification number of the first user is successfully authenticated” because, in Sullivan’s PVR, a user (“the first of the two users”) is allowed to access the instance of audio/visual content (“specific digital content”) in response to determining that the indication of the audio/visual content (“content identifier”) matches the indication of the user (“user identifier”), as described above, and the access code/password (“PIN,” *supra* [1e]) is successfully authenticated. For example, Sullivan’s PVR allows the thirteen-year-old to access a television show in response to determining that the television show is associated with the thirteen-year-old on an exception list and the user’s access code/password is authenticated. Sullivan, [0074], [0077], [0089]-[0090], [0099]-[0100]; Houh ¶105. Sullivan discloses rejecting “incorrect passwords” and disabling “access to the media” if the user enters an incorrect password too many times but allowing access to an authorized user upon “entering his or her password.” Sullivan, [0074]-[0075].

3. Dependent Claims

- a. **Claim 2: “The apparatus of claim 1, further comprising a rating policy database for storing rating based access controls for digital content of the digital library.”**

Sullivan or Sullivan and Craner teach the additional limitations of claim 2.

Houh ¶¶106-108.

Sullivan discloses creating and storing multiple user profiles “for individual users or groups of users.” Sullivan, [0088]. Sullivan’s exception lists are stored and associated with the stored content (“digital content of the digital library,” *supra* [1a]) for controlling access to the content. Sullivan, [0099]-[0100]. The PVR includes a “hard disk drive” and “prevent[s] unauthorized users from viewing restricted content in a number of ways.” Sullivan, [0100]-[0101]. A POSITA would have understood that the storage (e.g., on the hard disk drive) for the user profiles that include the acceptable content rating parameters and for the exception lists constitutes “a rating policy database for storing rating based access controls for digital content of the digital library.” Sullivan, [0088], [0099]-[0101]. Houh ¶107.

If Patent Owner argues Sullivan does not teach this, it would have been obvious in view of Craner. Craner teaches that a database was a well-known way to store “parental control settings and locks.” Craner, 20:47-54. A POSITA would

have been motivated to store the information about Sullivan's profiles and exception lists in a database on the PVR to facilitate determining whether the requested content is blocked and would have expected success, given the PVR's inclusion of a hard disk drive for storage. Houh ¶108.

b. Claim 3: "The apparatus of claim 2, further comprising a data port for exporting the policy database to another playback device."

Sullivan teaches the additional limitations of claim 3. Houh ¶¶109-111.

A POSITA would have found it obvious to include a data port on the PVR for exporting the policy database to another playback device. Houh ¶110.

Sullivan's PVR is a playback device. *Supra* [1pre]. Sullivan discloses that its content control system "may be implemented as sets of instructions resident in memory of one or more information appliances configured generally as described in FIG. 1." Sullivan, [0002], [0012], [0094]. The set of instructions can be stored in the memory of one device "and transmitted over a local area network or a wide area network ... when desired by the user." Sullivan, [0094]. This transmission would have involved one of the ports of the device's input/output system. Sullivan, [0032]; Houh ¶110. Sullivan also discloses using a PVR for "a single point of user control for parental locks for multiple audio and/or audiovisual devices." Sullivan, Abstract, [0002], [0095]. When the user selects the parental locks and presses

button 244, this “turn[s] on parental locks ... by mapping a user’s selections to each native parental control subsystem.” Sullivan, [0040].

Given Sullivan’s disclosure of a single device used to set the parental locks for multiple devices and its disclosure of transmitting the instructions over a network to other devices, a POSITA would have found it obvious to export the database of parental locks to another playback device. Houh ¶111. A POSITA would have been motivated to do so when acquiring a new playback device for the “entertainment system” to avoid having to configure this new device with the same parental locks already established. Sullivan, [0009]; Houh ¶111. This would have been beneficial, for example, to avoid duplicating parental lock settings on each device that has access to the same ratings enabled media. Sullivan, [0063]. Indeed, Sullivan discloses the desire to control “two or more[] parental control subsystems within an entertainment system.” Sullivan, [0009]. Moreover, Sullivan discloses that a “second content recorder should be enabled to block content bearing the restrictive rating information.” Sullivan, [0101]. This would have motivated a POSITA to export the policy database from the first PVR to a second PVR to ensure that the same policies are applied to content transferred to the second PVR. Houh ¶111. Given Sullivan’s disclosure of the desire and ability to transmit data via several ports, a POSITA would have reasonably expected success in doing so. Houh ¶111.

4. Independent Claim 4

- a. [4pre]: “A method in a computing system for creating specific rating policies for digital media access, the method comprising:”**

If limiting, Sullivan and Leung teach [4pre]. Houh ¶¶112-113.

Sullivan discloses implementing its PVR using a “hardware system 100” (“computing system”) that allows setting ratings-based parental locks and creating exception lists associated content on the PVR. Sullivan, [0031]-[0033], [0039]-[0040], [0046]-[0051], [0053], [0088]-[0089], [0099]-[0100]. As discussed in Section VI.A.1.a, it would have been obvious to implement Sullivan’s ratings-based parental locks using Leung’s V-chip. Houh ¶113. The exception lists, for example, are “specific rating policies for digital media access” on the PVR. *Supra* [1a]; Houh ¶113.

- b. [4a]: “under control of the computing system having a memory and a processor, performing the acts of:”**

Sullivan teaches [4a]. Houh ¶¶114-115.

Sullivan discloses implementing its PVR using the “hardware system 100,” which includes “a central processing system processor 102” and a “main memory 104” that “provides storage of instructions and data for programs executing on the central processing system 102,” as Figure 1 shows. Sullivan, [0031]; *see also id.*, [0033], [0094]. Sullivan’s PVR, under the control of this hardware system having

the memory and the processor, performs the functions discussed for [4b]-[4j].

Houh ¶115.

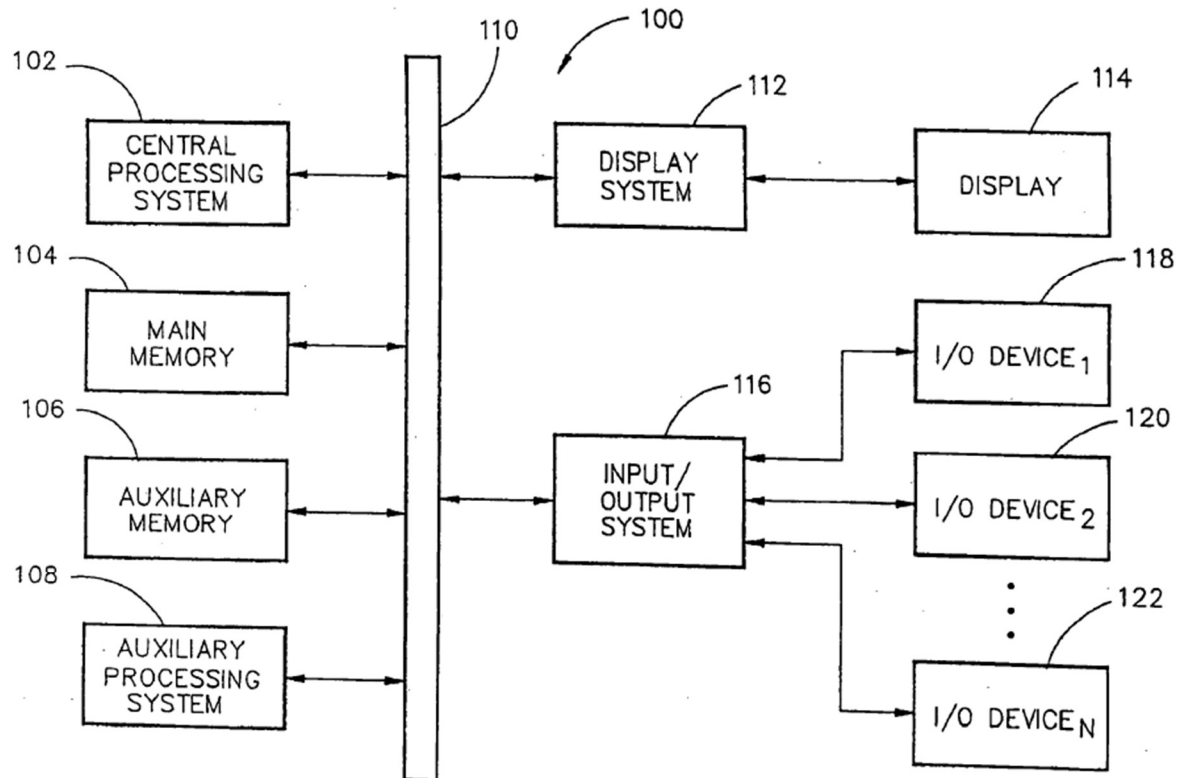


FIG. 1

Sullivan, FIG. 1.

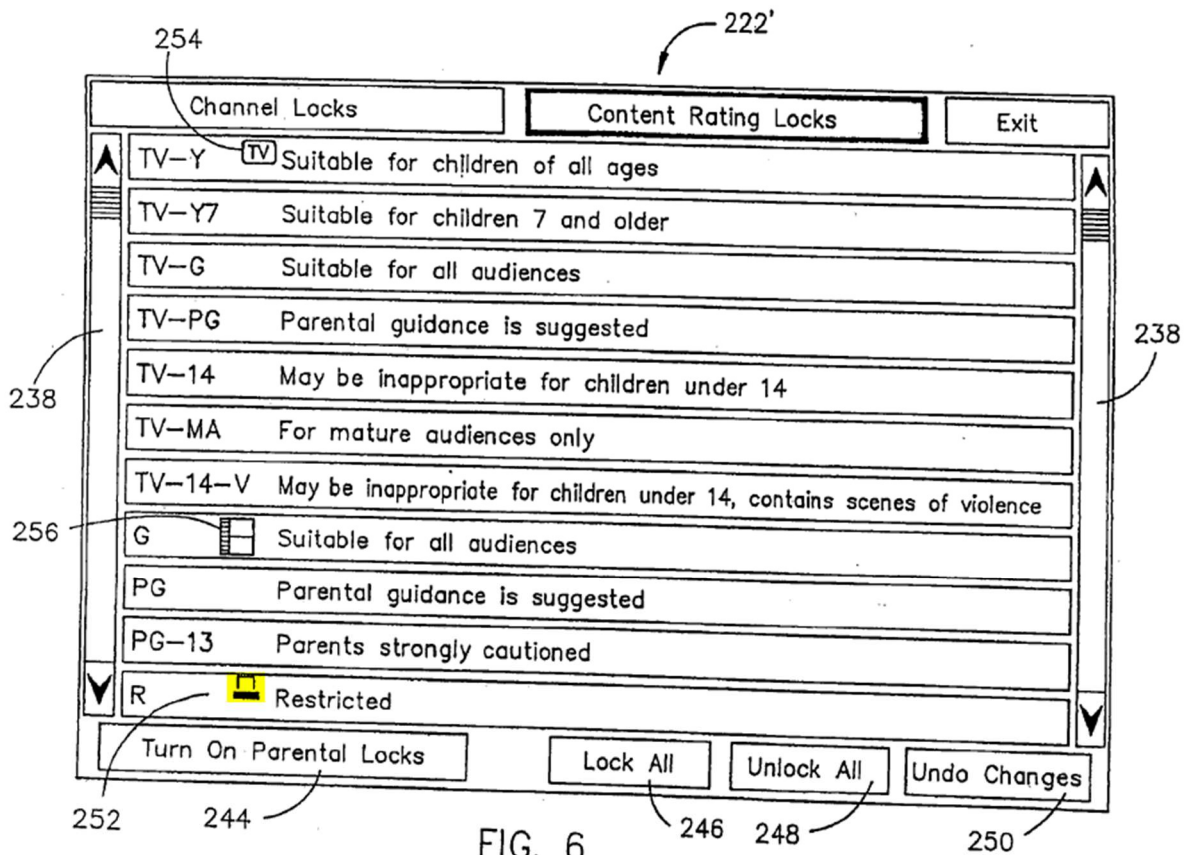
c. [4b]: “retrieving media information from the memory comprising a rating based media access policy for a digital content;”

[4c]: “displaying the rating based media access policy to a user;”

Sullivan teaches [4b] and [4c]. Houh ¶¶116-117.

Sullivan discloses “retrieving media information from the memory comprising a rating based media access policy for a digital content” and

“displaying the rating based media access policy to a user” because, after a user selects “the parental locks feature” to access the “parental locks interface,” the system retrieves from memory and displays “previously saved user settings or profiles” in the parental locks interface and gives the user “an option of selecting one.” Houh ¶117; Sullivan, [0046]-[0048]; *see also id.*, [0064]. Sullivan discloses “For example, Sullivan may display “a visual indication,” below, of the “ratings that have been selected to be locked.” Sullivan, [0041], [0053], [0072]-[0074], [0077], FIG. 6.



Sullivan, FIG. 6 (annotated).

- d. [4d]: “receiving from the user a first rating based access control policy override action for a first viewer and a second, different, rating based access control policy override action for a second viewer with respect to a same specific digital content,”**

Sullivan and Leung teach [4d]. Houh ¶¶118-125.

Sullivan discloses “receiving from the user a first rating based access control policy override action for a first viewer” with respect to a “specific digital content.” Houh ¶119. Sullivan’s television content stored in the PVR’s hard disk drive is a specific digital content. Sullivan, [0096]-[0100]; *supra* [1pre]. Sullivan discloses that the PVR receives from an authorized user a request to add a first viewer (e.g., a thirteen-year-old child) to an exception list associated with stored content that would ordinarily be blocked from the first viewer based on its rating and the content control system’s previously set acceptable content rating parameters (first rating based access control policy override action for a first viewer). Sullivan, [0072]-[0074], [0099]-[0100]; Houh ¶119.

A POSITA would have found it obvious to combine Sullivan and Leung to create a separate exception list that *blocks* access to associated content for identified viewers and receiving “a second, different, rating based access control policy override action for a second viewer with respect to a same specific digital content.” Houh ¶120. Similar to Sullivan’s exception lists, Leung uses “user

programmable enable override lists and blocking override lists.” Leung, [0052].

The blocking override list includes “the titles of television programs” that will result in the program being blocked despite having a rating that would not normally be blocked. Leung, [0054]-[0055], [0057], [0088]. An authorized viewer may access and edit this override list. Leung, [0097]. Figure 1, below, depicts the operation of Leung’s override system, including how a program that would otherwise be **allowed** based on its rating is **blocked** based on its inclusion on the override list. Leung, [0053]-[0054].

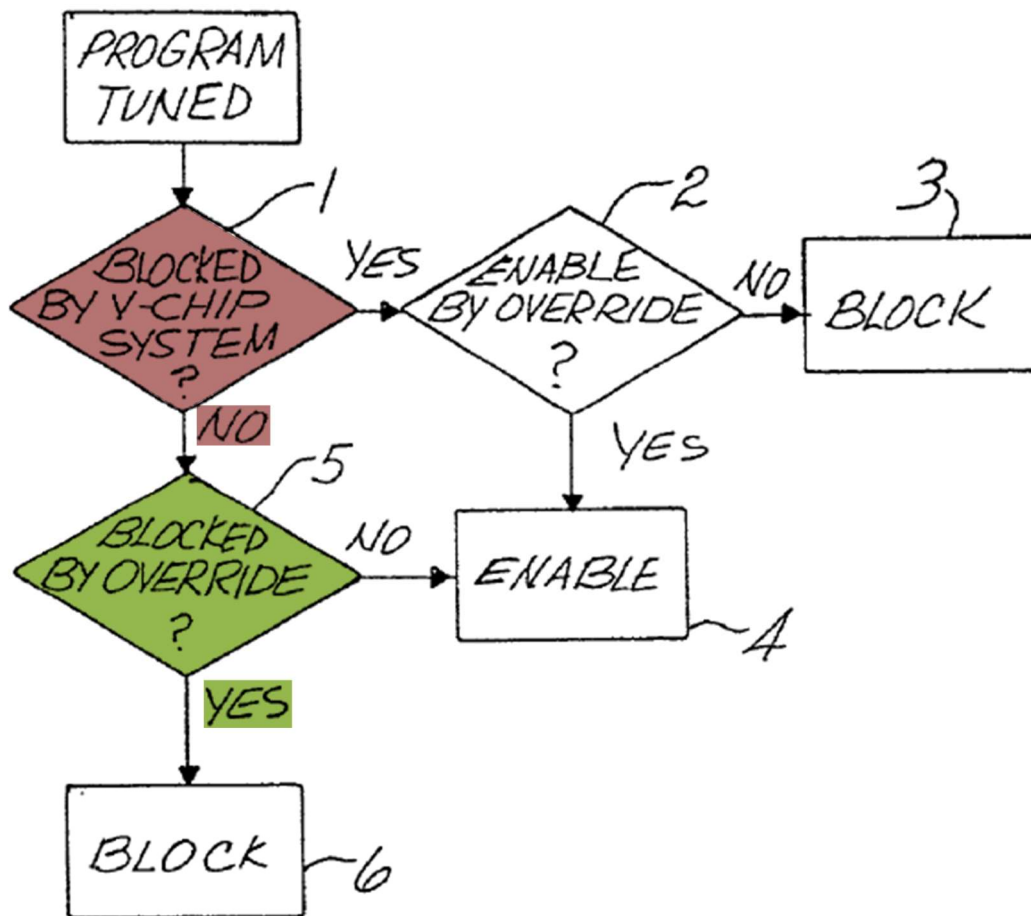


Fig. 1

Leung, FIG. 1 (annotated).

A POSITA would have been motivated to combine Sullivan and Leung to create a separate exception list associated with the same instance of stored audio/visual content that blocks users identified on the list who would otherwise be allowed to access the content based on its rating and that user's acceptable content rating parameters. Sullivan, [0072]-[0074], [0088]-[0089], [0099]-[0100]; Leung,

[0052]-[0055], [0057]; Houh ¶121. As Sullivan recognizes, a parent “may feel that a content rating for content the user has viewed may not be stringent enough, or conversely, too stringent, for sensitive users such as children, for whom access to the content is controlled by the user.” Sullivan, [0006]; Houh ¶121. Creating this second kind of exception list would have been desirable because, for one instance of saved content, a parent may feel that its content rating is too stringent for the first viewer who is blocked from accessing it based on that user’s lock levels and may feel that it is not stringent enough for another, second viewer (e.g., “Mark,” “Sarah,” or “Stephen”) who is permitted access based on that user’s lock levels. Sullivan, [0090], FIG. 15; Houh ¶121.

A POSITA would have been motivated to provide the ability for a parent, upon viewing such content, to either allow *or* block a particular child’s access to that content without changing that user’s acceptable content rating parameters. Houh ¶122. Indeed, Sullivan already discloses similar functionality, where an authorized user wanting to allow or block “the television program currently being viewed” can select a particular user profile for this action, resulting in that user’s parental lock levels being adjusted based on that program’s rating. Sullivan, [0090]-[0092]; Houh ¶122.

Because Sullivan discloses an exception list for allowing particular users access to otherwise blocked content and Leung teaches a blocking override list for

otherwise allowed content, a POSITA would have viewed an exception list for blocking access to content for particular users as the application of a known technique (the creation of an exception list) to improve Sullivan's content control system in the same way as its exception list for allowing access to content. Houh ¶123. Such a combination would have provided parents greater "flexibility and granularity" in their control of their children's access to stored content, which was known to be desirable. Sullivan, [0090]; Craner, 12:41-43; Houh ¶123.

A POSITA would have reasonably expected success in such a combination. Sullivan already discloses an exception list for allowing access. Sullivan, [0099]-[0100]. And contemporaneous references like Craner teach blocking specific programs for each user profile. Craner, 11:48-54, 12:7-12, 12:16-20. Accordingly, combining Sullivan and Leung would have required only conventional programming techniques to modify Sullivan's existing exception list disclosure for the purpose of blocking users from accessing content that would otherwise be allowed in a similar way to Leung's blocking override list. Houh ¶126.

Additionally, as discussed in Section VI.A.1.b, Sullivan and Leung render obvious modifying Sullivan's exception list associated with the requested content to allow a parent to specify different media ratings for multiple users if the parent disagrees with the original media rating as it pertains to each user. Sullivan, [0006]-[0007], [0095]-[0100]; *supra* [1c]; Houh ¶125. Each different media rating

in the exception list constitutes a different rating based access control policy override action for the corresponding user. Houh ¶125.

- e. **[4e]: “wherein the first viewer and second viewer are separate and distinct from the user from which the override actions are received, and”**

Sullivan teaches [4e]. Houh ¶126-127.

Sullivan’s PVR receives the generated exception lists (“override actions”) from “[a]n authorized user (e.g. a parent or guardian),” who is “separate and distinct from” the viewers (e.g., the seven-year-old and thirteen-year-old) whose profiles the authorized user controls. Sullivan, [0088]-[0090], [0099]-[0100], FIG. 15; Houh ¶127.

- f. **[4f]: “wherein the first viewer is associated with a first authentication code unique to the first viewer and the second viewer is associated with a second authentication code unique to the second viewer;”**

Sullivan teaches [4f]. Houh ¶¶128-129.

Each of Sullivan’s users has a “unique password” (authentication code) associated with their profile. Sullivan, [0074], [0077], [0089]-[0090], [0099]; *supra* [1d]; Houh ¶129.

- g. **[4g]: “storing the first and second policy override actions in a rating policy repository wherein future playback of the**

**digital content is allowed or blocked
consistent with the stored policy override
action, and”**

Sullivan and Leung teach [4g]. Houh ¶¶130-132.

As discussed for [4d], it would have been obvious to combine Sullivan and Leung to receive generated exception lists (“first and second policy override actions”) at the PVR. Houh ¶131. Sullivan discloses that each “exception list is stored” on the PVR and “associated with the stored content for controlling access to the content.” Sullivan, [0099]-[0100]; Houh ¶131.

The memory on the PVR (e.g., the hard disk drive) where the exception lists are stored constitutes “a rating policy repository” because it contains the first and second policy override actions. *Supra* [4d]; Houh ¶132. “[F]uture playback of the digital content” stored on the PVR and associated with each exception list “is allowed or blocked consistent with the stored” exception list (“policy override action”). Sullivan, [0099]-[0100]; Houh ¶132. For example, the PVR’s content control system applies the exception list’s access policy whenever a user identified on the exception list attempts to access the associated content. Sullivan, [0074], [0077], [0089], [0099]-[0101]; Leung, [0053]-[0054]; Houh ¶132.

- h. [4h]: “wherein the first viewer is allowed to access the specific digital content based upon the first authentication code and the second viewer is blocked from access to**

**the specific digital content based upon the
second authentication code,”**

Sullivan and Leung teach [4h]. Houh ¶¶133-135.

Sullivan discloses that “the first viewer is allowed to access the specific digital content based upon the first authentication code.” *See* [1d]; Houh ¶134.

Sullivan and Leung teach that “the second viewer is blocked from access to the specific digital content based upon the second authentication code.” As discussed for [4d], it would have been obvious to combine Sullivan and Leung to receive an exception list associated with an instance of audio/visual content saved on the PVR denoting a second viewer who is blocked from accessing the content and who would otherwise be allowed to access the content. Houh ¶135. If the second viewer attempts to access the associated content, that user’s “unique password” (“second authentication code”) would result in Sullivan’s system, modified in view of Leung, blocking access to that content if the second viewer appears on the exception list for blocking access, consistent with Sullivan’s disclosure that “unauthorized viewers ... who do not possess the necessary password” cannot view blocked content. Sullivan, [0074], [0099]-[0100]; Houh ¶135. A POSITA would have been motivated to block the second viewer’s access to content whose rating the parent has deemed not “stringent enough” for that user. Sullivan, [0006]; Houh ¶135. A POSITA would have reasonably expected success

as discussed for [4d]. Moreover, implementing this functionality would have required a POSITA to apply the same conventional techniques used in Sullivan's exception list for allowing access. Houh ¶135.

- i. **[4i]: “wherein the first authentication code comprises a personal identification number (PIN), and”**

[4j]: “wherein the first of the two viewers is allowed to access the specific digital content in response to determining that a content identifier of the specific digital content matches a user identifier of the first viewer and the personal identification number of the first viewer is successfully authenticated.”

Sullivan and Craner teach [4i] and [4j] as discussed for [1e] and [1g]. Houh ¶¶136-137.

5. Dependent Claims

- a. **Claim 5: “The method of claim 4 further comprising validating the authentication codes of the first viewer and the second viewer.”**

Sullivan teaches the additional limitations of claim 5. Houh ¶¶138-139.

Sullivan teaches that, if a user selects content blocked “because its content rating exceeds the rating threshold,” the user must enter an access code/password “to access the blocked content.” Sullivan, [0073]-[0074], [0077]. “[U]nauthorized viewers, such as children, who do not possess the necessary password” cannot

access the blocked content. Sullivan, [0074]; *supra* [1g], [4h]. Sullivan also discloses that, when multiple user profiles exist, each user “enter[s] his or her user identification [(e.g., “a user name and password”)] via the user interface to access content.” Sullivan, [0088]-[0090], [0099]; Houh ¶139. “[I]f incorrect passwords are entered a predetermined number of times, the system may be instructed to disable access to the media.” Sullivan, [0075]. Accordingly, Sullivan discloses, or at least renders obvious, “validating the authentication codes of the first viewer and the second viewer.” Houh ¶139.

b. Claim 6: “The method of claim 4, wherein the first and second authentication codes comprise a personal identification number (PIN).”

For the same reasons discussed for [1e], it would have been obvious to implement each user’s password, including “the first and second authentication codes” as a PIN. Houh ¶140.

c. Claim 7: “The method of claim 5, wherein the authentication codes comprise biometric information.”

Sullivan and Craner teach the additional limitations of claim 7. Houh ¶¶141-144.

Similar to Sullivan, Craner discloses authenticating users “using a standard username and password combination.” Craner, 11:48-58; Sullivan, [0089]-[0090].

Alternatively, Craner discloses authenticating users with “a verification module” based on “voice, iris, or fingerprint verification.” Craner, 11:54-58. Voice, iris, and fingerprint verification each disclose authentication codes comprising biometric information. Houh ¶142.

A POSITA would have been motivated by Craner to implement Sullivan’s access codes/passwords using biometric information. Houh ¶143. Craner explains that using biometric information allows access to be granted “without the use of a manual parental control access code entry”—something especially useful for children, whom Sullivan envisions as users. Craner, 9:17-30; Houh ¶143. Moreover, using biometric information would have increased security because “[i]t is easy for the children” to learn another’s PIN by watching them “work the remote control.” Novack, [0009].

A POSITA would have reasonably expected success implementing Sullivan’s access codes/passwords using such that the authentication codes for the first and second users comprise biometric information because this would have involved only conventional techniques. Houh ¶144. Using biometric information with a remote control was a well-known technique. Novack, [0013]-[0014], [0030]-[0031]; Houh ¶144.

d. Claim 8: “The method of claim 4, further comprising displaying the media

**information, wherein the media
information comprises a media rating.”**

Sullivan teaches the additional limitations of claim 8. Houh ¶¶145-150.

As discussed for [4b] and [4c], Sullivan teaches “retrieving media information from the memory comprising a rating based media access policy for a digital content” and “displaying the rating based media access policy to a user” because Sullivan’s PVR displays the “parental locks interface” including the “user profiles.” Houh ¶146. As Sullivan explains, a user may “open a preexisting user profile” and, through the parental locks interface, view “the level of parental locking,” which includes “the material and/or channels to be locked.” Sullivan, [0045], [0048]. Sullivan’s parental locks interface is illustrated in Figure 4. As shown, Sullivan’s interface includes a number of “TV or movie rating[s],” and “a user may select particular ratings to lock and unlock.” Sullivan, [0039]. Thus, Sullivan’s interface displays “media information [that] comprises a media rating.” Houh ¶146.

If Patent Owner argues Sullivan does not teach “displaying ... a media rating,” a POSITA would have been motivated to include a media rating in Sullivan’s parental locks interface based on Leung. Houh ¶147. Leung describes a “parental control user interface” that allows a parent to “override” an existing rating “for individually selected television programs.” Leung, Abstract, [0076]-

[0077]. This interface is described in both a TV mode and a GUIDE mode.

Leung's TV mode, shown in Figure 24, displays "the current rating set by the viewer," as in Sullivan. Leung, [0121]-[0122]. "Each of these rating factors can be individually activated or deactivated" by the parent through the interface. Leung, [0122].

The interface is a rectangular box divided into several sections. At the top, it says "SET V-CHIP" followed by two checkboxes labeled "ON" and "OFF". Below this, there are two buttons: "TV RATINGS" and "MOVIE RATINGS". The "TV RATINGS" button is highlighted with a yellow background. Below the buttons, it says "BLOCKS SHOWS RATED HIGHER THAN:" followed by a yellow bar containing the text "TV-PG PARENTAL GUIDANCE". Below this, it says "AND BLOCKS:". There are four checkboxes with labels: "VIOLENCE" (with a handwritten "132" to its left), "LANGUAGE", "SEXUAL SITUATIONS", and "DIALOGUE". The "LANGUAGE", "SEXUAL SITUATIONS", and "DIALOGUE" checkboxes are marked with an 'X'. At the bottom, it says "TO PERSONALIZE YOUR TV VIEWING, PRESS V-CHIP PLUS+/BLOCK" with a handwritten "134" to its right. Below this, there are two rows of controls: the first row has "Δ∇ . TO MOVE" and "◁ ▷ CHANGE/SELECT"; the second row has "VCHIP+" and "TO EXIT".

Fig. 24

Leung, FIG. 24 (annotated).

Leung also describes the "GUIDE mode" for its interface. Leung, [0049], [0152], [0174]. As shown in Figure 51, the interface lists content, including media

ratings for each content. From this interface, “[i]ndividual shows or entire channels may be blocked.” Leung, [0174].



FIG. 51

Leung, FIG. 51.

From Leung, a POSITA would have been motivated to implement Sullivan’s parental locks interface to include a media rating for each content because Leung teaches that an interface (its GUIDE mode) including media ratings for each

content is an alternative to an interface that, like Leung's TV mode and Sullivan's parental locks interface, lists media ratings. Houh ¶150. A POSITA would have been motivated at least by Leung's explanation that including media ratings for each content in the interface allows "[i]ndividual shows or entire channels" to be blocked, in addition to blocking based on ratings. Leung, [0174]; Houh ¶150. A POSITA would have reasonably expected success because Sullivan discloses that the PVR stores this information, so including a media rating for each instance of content would have required a POSITA to apply only conventional techniques to display information stored in memory. Sullivan, [0096]-[0100]; Houh ¶150.

e. Claim 9: "The method of claim 4, further comprising displaying the media information, wherein the media information comprises a media owner."

Sullivan or Sullivan and Leung teach the additional limitations of claim 9. Houh ¶¶151-155.

As discussed for [4b] and [4c], Sullivan teaches "retrieving media information from the memory comprising a rating based media access policy for a digital content" and "displaying the rating based media access policy to a user" because Sullivan's PVR displays the "parental locks interface" including the "user profiles." Houh ¶152. Through Sullivan's parental locks interface, "a user may select particular ratings to lock and unlock." Sullivan, [0039], [0045]. Sullivan also

discloses a user setting parental locks using a “channel lock overlay” that displays media information comprising a media owner because it displays the “channel name” or “channel logo” corresponding to channels that may be blocked. Sullivan, [0038], [0047]; Houh ¶152. One channel lock overlay is depicted in Figure 3.

Sullivan teaches that, “if the user opens a preexisting profile with an intent to modify that profile,” Sullivan’s system would retrieve the media information comprising a media owner from memory and display the current settings in an overlay like the one below. Sullivan, [0047]-[0050]; Houh ¶152.

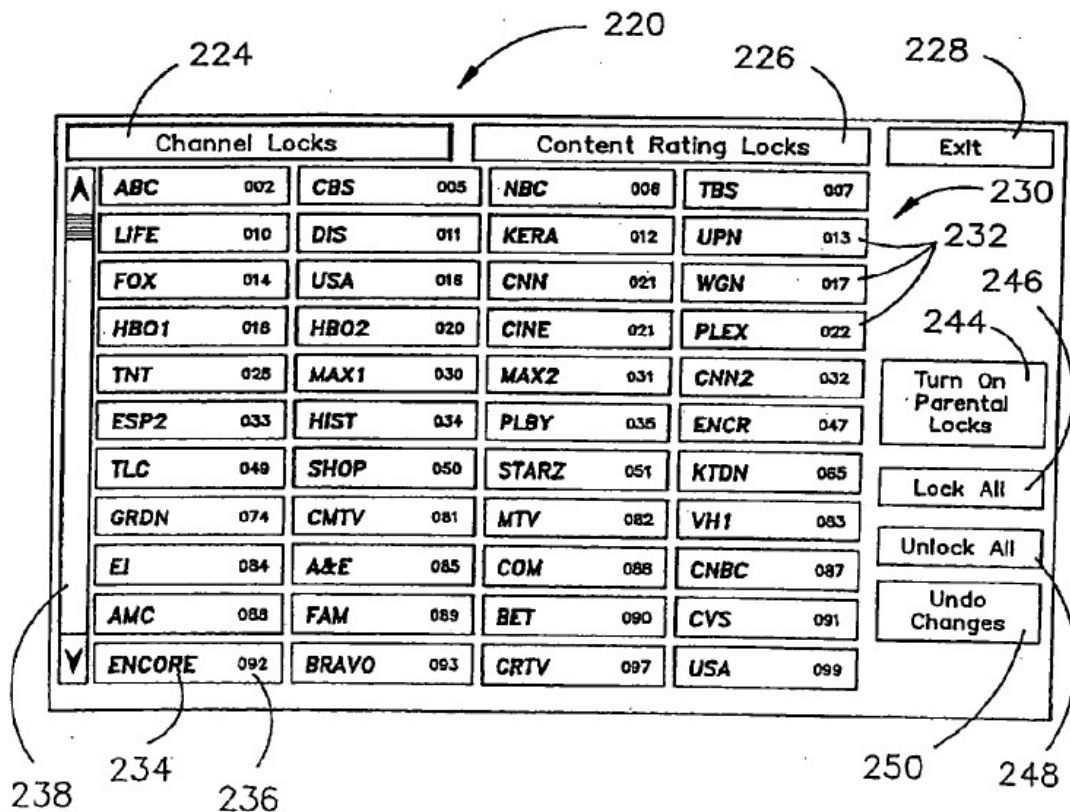


FIG. 3

Sullivan, FIG. 3.

Alternatively, a POSITA would have been motivated to include “a media owner” in Sullivan’s parental locks interface based on Leung. Houh ¶153. As explained for claim 8, Leung describes a “parental control user interface” that allows a parent to “override” an existing rating “for individually selected television programs.” Leung, Abstract, [0076]-[0077]. And, as explained for claim 8, Leung’s parental control interface is described in both a TV mode (*see, e.g.*, Leung, [0121]-[0122], FIG. 24) and a GUIDE mode (*see, e.g.*, Leung, [0152], [0174], FIG. 51).

As shown in Figure 51, in Leung’s GUIDE mode, the interface lists content, including a media owner for each content. For example, the media owner of the content “Columbo” is shown to be “FOX,” while the media owner of the content “Young Philadelphians” is shown to be “AMC.” Leung, FIG. 51. From this interface, Leung explains, “[i]ndividual shows or entire channels may be blocked.” Leung, [0174].



FIG. 51

Leung, FIG. 51.

From Leung, a POSITA would have been motivated to implement Sullivan's parental locks interface to include a media owner for each content because Leung teaches that an interface (its GUIDE mode) including media owners for each content is an alternative to an interface that, like Leung's TV mode and Sullivan's parental locks interface, lists only media ratings. Houh ¶155. A POSITA would have been motivated at least by Leung's explanation that including media owners

for each content in the interface allows “[i]ndividual shows or entire channels” to be blocked, in addition to blocking based on ratings. Sullivan, [0174]; Houh ¶155. A POSITA would have reasonably expected success because Sullivan’s system already employs “channels” associated with content to implement the parental locks, so including a channel (media owner) for each instance of content would have required a POSITA to apply only conventional techniques to display information known to the system. Sullivan, [0004]-[0005] (acknowledging that “existing content control systems” employ “channel locks”), [0037]-[0038], [0040]-[0043], FIGS. 3, 5; Houh ¶155.

f. Claim 10: “The method of claim 4, wherein the first policy override action comprises modifying media access for the first viewer and the second policy override action comprises modifying media access for the second viewer.”

As explained for [4d], Sullivan’s addition of a first viewer to an exception list for an audio/visual content discloses a “first ... policy override action.” This addition to the exception list “modif[ies] media access for the first viewer” because it “allow[s]” the first viewer to “view an instance of audio/visual content ... which may ordinarily be blocked from the [first viewer’s] view.” Sullivan, [0099]-[0100].

And, as explained for [4d], Sullivan’s addition of a second viewer to the exception list for an audio/visual content (as rendered obvious by Sullivan and

Leung) discloses a “Sullivan and Leung teach the “second, different, ... policy override action.” This addition to the exception list “modif[ies] media access for the second viewer” because it blocks the second viewer from viewing the audio/visual content. Sullivan, [0099]-[0100].

g. Claim 11: “The method of claim 4, wherein the first policy override action comprises modifying media access for a group that includes the first viewer.”

As explained for [4d], Sullivan discloses a “first ... policy override action” because Sullivan discloses that the first viewer may be added to an “exception list” associated with “an instance of audio/visual content.” Sullivan, [0099]-[0100]. Sullivan teaches that this exception list “modif[ies] media access for a group that includes the first viewer” because Sullivan envisions that “parental lock levels” reflected in the exception list may apply to “each user or *group of users*.” Sullivan, [0090]-[0092], FIG. 15 (emphasis added). Accordingly, Sullivan envisions creating “profiles” for individuals or groups and that “acceptable content rating parameters” are “set specifically for that user or *group of users*.” Sullivan, [0088] (emphasis added). For example, parameters may be set “for different children (or age groups).” Sullivan, [0047]. Accordingly, Sullivan’s teaching of an exception list likewise allows parents to add one of the groups previously discussed that includes

the first viewer (e.g., “Children”). Sullivan, [0090], [0099]-[0100], FIG. 15; Houh ¶158.

6. Independent Claim 12

- a. **[12pre]: “A method in a computing system for rating based media access policy enforcement, the method comprising:”**

If limiting, Sullivan teaches [12pre] as discussed for claim 1. Houh ¶159. Sullivan’s PVR, for example, is “a computing system” that implements “a method ... for rating based media access policy enforcement” for each user of the PVR. Sullivan, [0031]-[0033], [0046]-[0051], [0053], [0074], [0077], [0088]-[0090], [0099]-[0101]; *supra* [1b]-[1g].

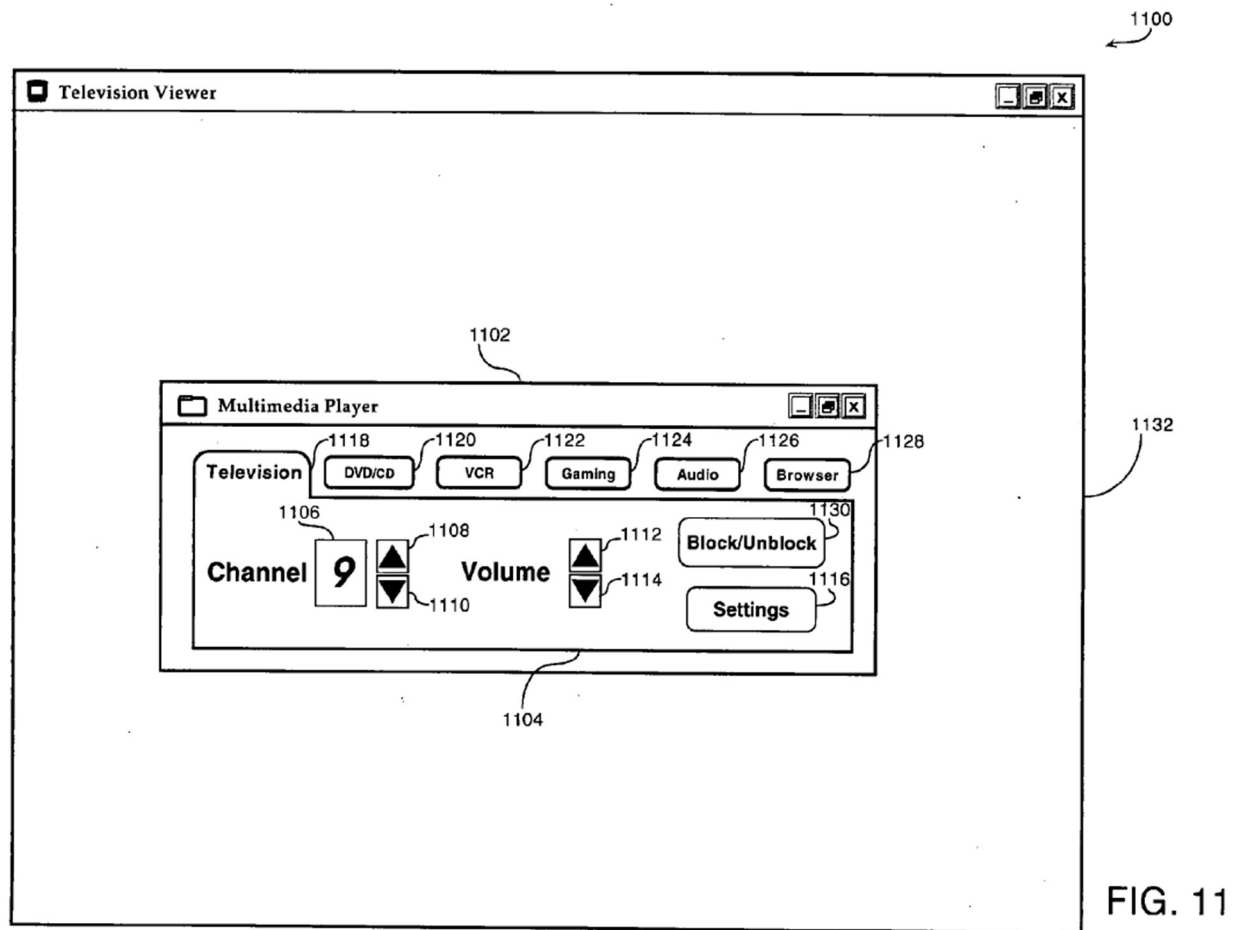
- b. **[12a]: “under control of a video playback device having a V-chip that specifies default rating based access policy, performing the acts of:”**

Sullivan and Leung teach [12a] for the reasons discussed in Section VI.A.1.a and for [1pre]-[1a]. Houh ¶160. Sullivan’s PVR, implemented with Leung’s V-chip, is a “video playback device having a V-chip that specifies [a] default rating based access policy[.]” *Supra* Section VI.A.1.a, [1pre]-[1a].

- c. **[12b]: “displaying metadata;”**

Sullivan or Sullivan and Leung teach [12b]. Houh ¶¶161-166.

Sullivan discloses displaying “an on-screen control panel 1102 for controlling access to media by the information appliance” that includes “display fields” (e.g., “Channel”) and control buttons, which represent “controls of the information appliance or ... peripheral devices attached thereto.” Sullivan, [0066]. Buttons in the user interface “change the contents of region or window 1104 so that the controls provided therein are suitable for controlling functions of the information appliance and/or peripheral devices used to access the media.” Sullivan, [0067]. As shown below, which shows a television viewing application, Sullivan’s control panel displays the selected channel number. Sullivan, [0072], FIG. 11; Houh ¶162. While only controls for the “Television” are illustrated, Sullivan also envisions displaying controls for a “DVD/CD,” “VCR,” “Gaming,” “Audio,” and “Browser.” Sullivan, FIG. 11; Houh ¶162.



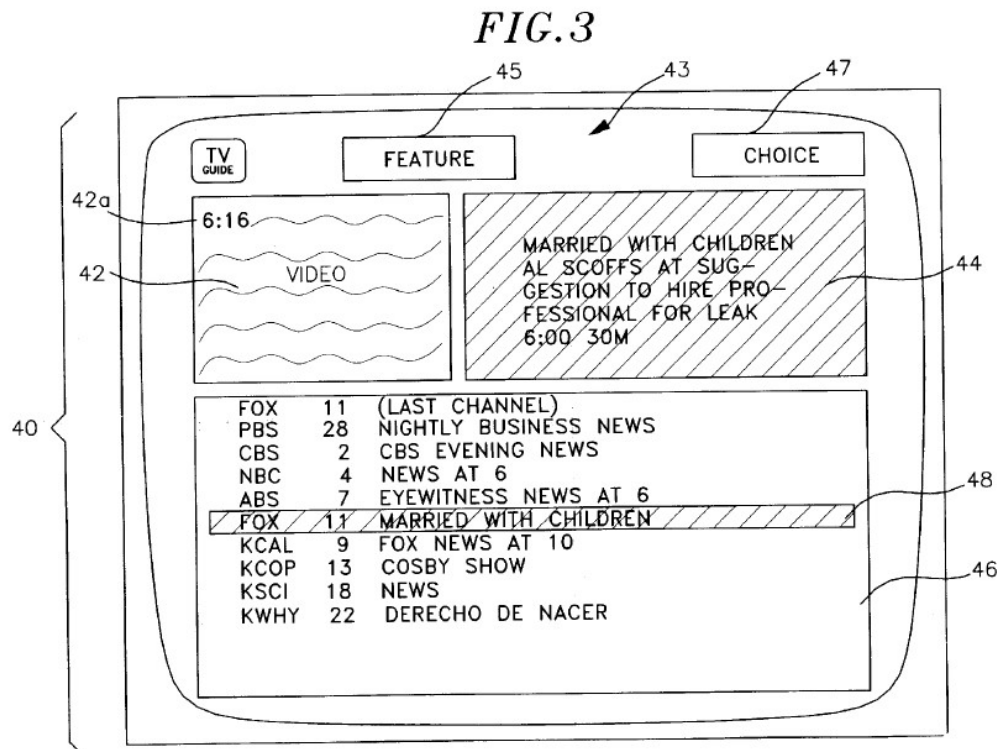
Sullivan, FIG. 11.

A POSITA would have understood that, when using Sullivan's PVR, the user interface would display the PVR-viewing application, through which a user could select specific content to view. Sullivan, [0095]-[0101]; Houh ¶163. Moreover, the PVR-viewing application would include selectable metadata corresponding to recorded television programs stored at the PVR, to aid a user in selecting content. Houh ¶163. Such a display of selectable metadata was a well-known way to implement controls suitable for controlling functions of the PVR

used to access the media stored thereon. Sullivan, [0067], [0095]-[0101]; Barton, [0093]-[0094], [0098], FIGS. 8-10; Baumgartner, FIG. 20a; Houh ¶163.

If Patent Owner argues Sullivan does not disclose this, Sullivan and Leung would have rendered it obvious. Houh ¶164. Leung, through its incorporation by reference of U.S. Application No. 08/744,399, which issued as U.S. Patent No. 6,477,705 (“Yuen”)², discloses displaying “television program listings” and allowing a viewer to select a television program with a cursor. Leung, [0099]; Yuen, Abstract; *see also* Leung, [0156], FIG. 41 (depicting metadata for user selection). Figure 3, below, displays metadata corresponding to program listings, including the titles and channels for available programs. Yuen, 6:9-14, 7:41-51, FIG. 3. A viewer uses a remote control to move an on-screen cursor, “highlight one of the program listings displayed,” and select the desired program to watch. Yuen, 2:35-42, 5:62-63, 6:18-29, 7:34-40, 11:23-25.

² Material incorporated by reference “is effectively part of the host document as if [it] were explicitly contained therein.” *Arbutus Biopharma Corp. v. ModernaTX, Inc.*, 65 F.4th 656, 662-63 (Fed. Cir. 2023).



Yuen, FIG. 3.

A POSITA would have been motivated to combine Sullivan and Leung to display metadata in an interface that lists the titles of available content on the PVR to facilitate playback of the desired program via selection of the listed metadata. Houh ¶165. Such a display of metadata was well known and would have been a beneficial and familiar user interface for users to easily navigate through and select from the available content on the PVR. Barton, [0093]-[0094], [0098], FIGS. 8-10; Baumgartner, FIG. 20a; Houh ¶165. A POSITA would have been motivated to consult similar user interfaces, like Leung's, that display metadata about the

available programs to inform the user what is available to view and enable a user to easily select the desired content. Houh ¶165.

A POSITA would have reasonably expected success in displaying metadata for selection because Sullivan already discloses displaying television channels to select, and the PVR includes a hard disk drive for storing television content “from a television receiver.” Sullivan, [0096]-[0100]; Houh ¶166. Given the prevalence of similar user interfaces, incorporating the display of metadata into Sullivan’s PVR user interface would have required applying only conventional techniques to access metadata associated with the available programs and display the metadata in a user interface that enables selection of metadata to watch the associated content. Houh ¶166.

- d. [12c]: “responsive to a first user selecting a media content from the displayed metadata, and responsive to determining that rating based access control configured to override the V-chip default rating based access policy is enabled:”**

Sullivan and Leung teach [12c] and subelements [12d]-[12g], addressed in the subsequent sections. Houh ¶¶167-171.

As discussed for [12b], Sullivan discloses or Sullivan and Leung would have rendered obvious a user interface displaying metadata corresponding to the recorded television programs, where a user could select media content from the

displayed metadata to view specific content. Sullivan, [0095]-[0101]; *supra* [12b]; Houh ¶168.

Sullivan and Leung teach “determining that rating based access control configured to override the V-chip default rating based access policy is enabled.” Houh ¶169. As discussed for [12a], it would have been obvious to incorporate Leung’s V-chip to implement Sullivan’s specified default rating based policy. Houh ¶169. Sullivan teaches that this specified default rating based access policy applies when enabled by the “Turn On Parental Locks” button but is overridden for content if the authorized user creates a corresponding exception list identifying users to whom the default rating based policy does not apply. Sullivan, [0040], [0074], [0077], [0088]-[0089], [0099]-[0100], FIG. 4; *supra* [4d].

Sullivan teaches that, when an authorized user creates or updates the parental locks settings, such as by creating an exception list, “the locks are applied” to the PVR’s content control system. Sullivan, [0046]-[0050], [0088]-[0089], [0099]-[0100]; Houh ¶170. After the locks are applied, “it is determined whether any changes were made,” and the changes are saved. Sullivan, [0050]. This teaches determining that rating based access control configured to override the V-chip default rating based access policy is enabled because the content control system determines that content-specific policies exist, overriding the specified

default rating based policy implemented using Leung's V-chip for the users identified on the associated exception list. Houh ¶170.

In response to the above determinations, Sullivan and Leung teach subelements [12d]-[12g]. Houh ¶171.

e. [12d]: “reading media information”

Sullivan teaches [12d] because, “upon receiving the user request” to view television content, Sullivan's system determines if the selected content is blocked, “because its content rating exceeds the rating threshold” set by the content control system. Sullivan, [0063], [0073]. To make this determination, the content control system reads media information, such as the stored rating of the selected content. Sullivan, [0073], [0096]-[0100]; *supra* Section VI.A.1.a; Houh ¶172.

f. [12e]: “reading a default rating based access policy action associated with the selected media content configured to override the V-chip default rating based access policy; and”

Sullivan and Leung teach [12e] for the reasons discussed in Section VI.A.1.b. Sullivan's exception lists are stored on the PVR's memory and associated with the content. Sullivan, [0099]-[0100]. To determine whether a user appears on the exception list, Sullivan's PVR reads the stored exception list, which (as explained above) is “a default rating based access policy action associated with the selected media content configured to override the V-chip default rating based

access policy.” Houh ¶173; *see also* Sullivan, [0073]-[0074], [0099]-[0100]. If the content control system determines that the content is blocked by default, the reads any exception list associated with the selected content to determine whether it identifies a user granted access to the otherwise blocked content. Sullivan, [0074], [0089]-[0090], [0099]-[0100]; Houh ¶173. Conversely, if the system determines that content is allowed by default, the modified content control system reads any exception list associated with the selected content to determine whether it identifies a user whose access to the otherwise allowed content has been blocked. *Supra* [4d]; Houh ¶173.

g. [12f]: “responsive to determining that an authentication code is required: validating an authentication code; and”

[12g]: “beginning playback of the media; and”

Sullivan teaches [12f] and [12g]. Houh ¶174. Sullivan teaches “determining that an authentication code is required” because Sullivan teaches that “[i]f the example content is blocked,” but the “exception list associated with” the content indicates the user “is allowed to access the content” anyway, this user can view the content upon entry of their associated access code/password. Houh ¶174; Sullivan, [0074], [0089]-[0090], [0099]-[0100]. Sullivan teaches “validating an authentication code” and “beginning playback of the media” because, as Sullivan

explains, “the content control system allows the information appliance to provide”
the selected content when a user given access to the content enters their access
code/password. Houh ¶174; Sullivan, [0077], FIG. 13.

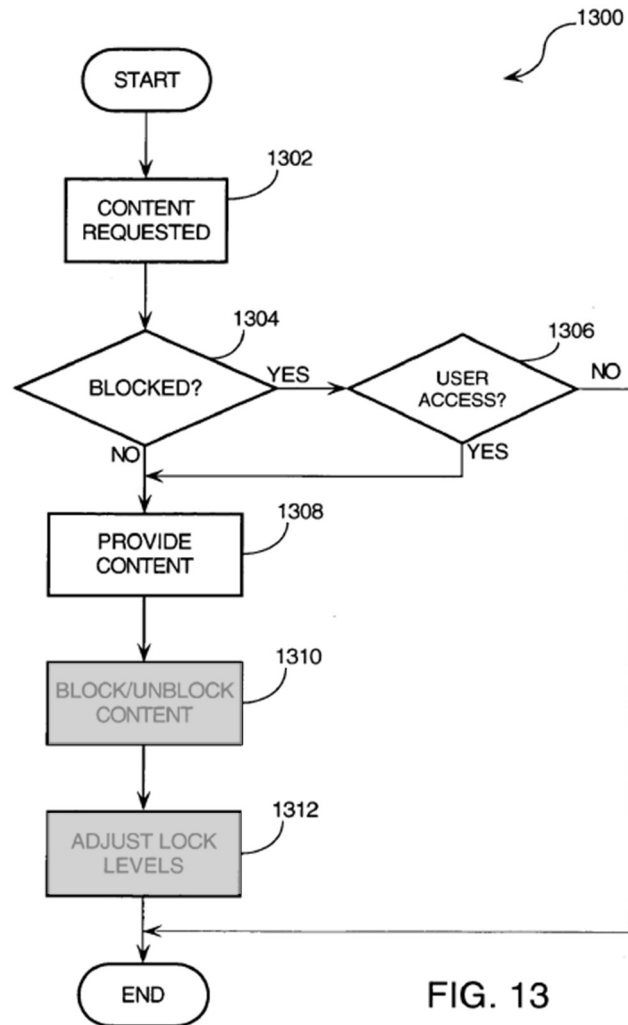


FIG. 13

Sullivan, FIG. 13 (annotated).

- h. [12h]: “responsive to a second different user selecting the same media from the displayed metadata: determining that an

**authentication code associated with the
second preventing playback of the media”**

Sullivan teaches [12h]. Houh ¶¶175-176.

Sullivan discloses that a seven-year-old and a thirteen-year-old have different passwords for accessing content on the PVR. Sullivan, [0099]. In Sullivan’s example, only the thirteen-year-old user has been added to an exception list allowing override access to a particular “TV-14 rated television program.” Sullivan, [0099]-[0100]. Sullivan also discloses configuring the user profiles so that the younger child has “more restrictive acceptable content rating parameters than would a teen-aged child.” Sullivan, [0088]. Accordingly, if the seven-year-old child (second different user) selects the same “TV-14 rated television program” from the displayed metadata, *supra* [12b], and enters their own password, Sullivan’s system prevents playback because the associated rating exceeds the second user’s acceptable rating parameters and the second user does not appear on the associated exception list. Sullivan, [0074], [0088]-[0089], [0099]-[0101]; Houh ¶176.

- i. **[12i]: “wherein the first and second users are not administrators of the rating based access control configured to override the**

V-Chip default rating based access policy,”

[12j]: “wherein the first authentication code comprises a personal identification number (PIN), and”

[12k]: “wherein the first of the two users is allowed to access the media content in response to determining that a content identifier of the media content matches a user identifier of the first user and the personal identification number of the first user is successfully authenticated.”

Sullivan teaches [12i]-[12k] as discussed for [4e], [1e], and [1g]. Houh

¶¶177-180.

7. Dependent Claims

- a. Claim 13: “The method of claim 12, wherein the authentication codes comprise personal identification numbers.”**

Sullivan and Craner teach the additional limitations of claim 13 for the reasons discussed for [1e]. Houh ¶181.

- b. Claim 14: “The method of claim 12, wherein the authentication codes comprise biometric information.”**

Sullivan and Craner teach the additional limitations of claim 14, as explained for claim 7. Houh ¶182.

c. Claim 15: “The method of claim 12, wherein the default rating based access policy action is to deny access.”

Sullivan teaches the additional limitations of claim 15. Houh ¶183.

As discussed for [12e], Sullivan’s exception list is “a default rating based access policy action.” Houh ¶184. The exception list serves “to deny access” because users on the exception list are only granted access to the associated content if they enter their unique password, thereby preventing access from other users, like the seven-year-old (*supra* [12h]), who are not on the list. Sullivan, [0089], [0099]-[0101]; Houh ¶184.

d. Claim 16: “The method of claim 12, wherein the media information comprises a rating.”

Sullivan teaches the additional limitation of claim 16. Houh ¶185.

As discussed for [12d], Sullivan discloses “reading media information,” such as the stored rating of the selected content. Sullivan, [0073]-[0074], [0099]-[0100]; *supra* [12d]; Houh ¶186.

e. Claim 17: “The method of claim 12, wherein the media information comprises a genre.”

Sullivan and Leung teach the additional limitations of claim 17. Houh ¶¶187-190.

As discussed for [12d], Sullivan discloses “reading media information.”

Leung discloses that a parent “may block all shows in a subcategory,” such as “Horror.” Leung, [0175]. Figure 54, below, discloses an interface allowing a parent to view genres of movie categories and press a button “to block all Horror Movies.” Leung, [0175], FIG. 54.

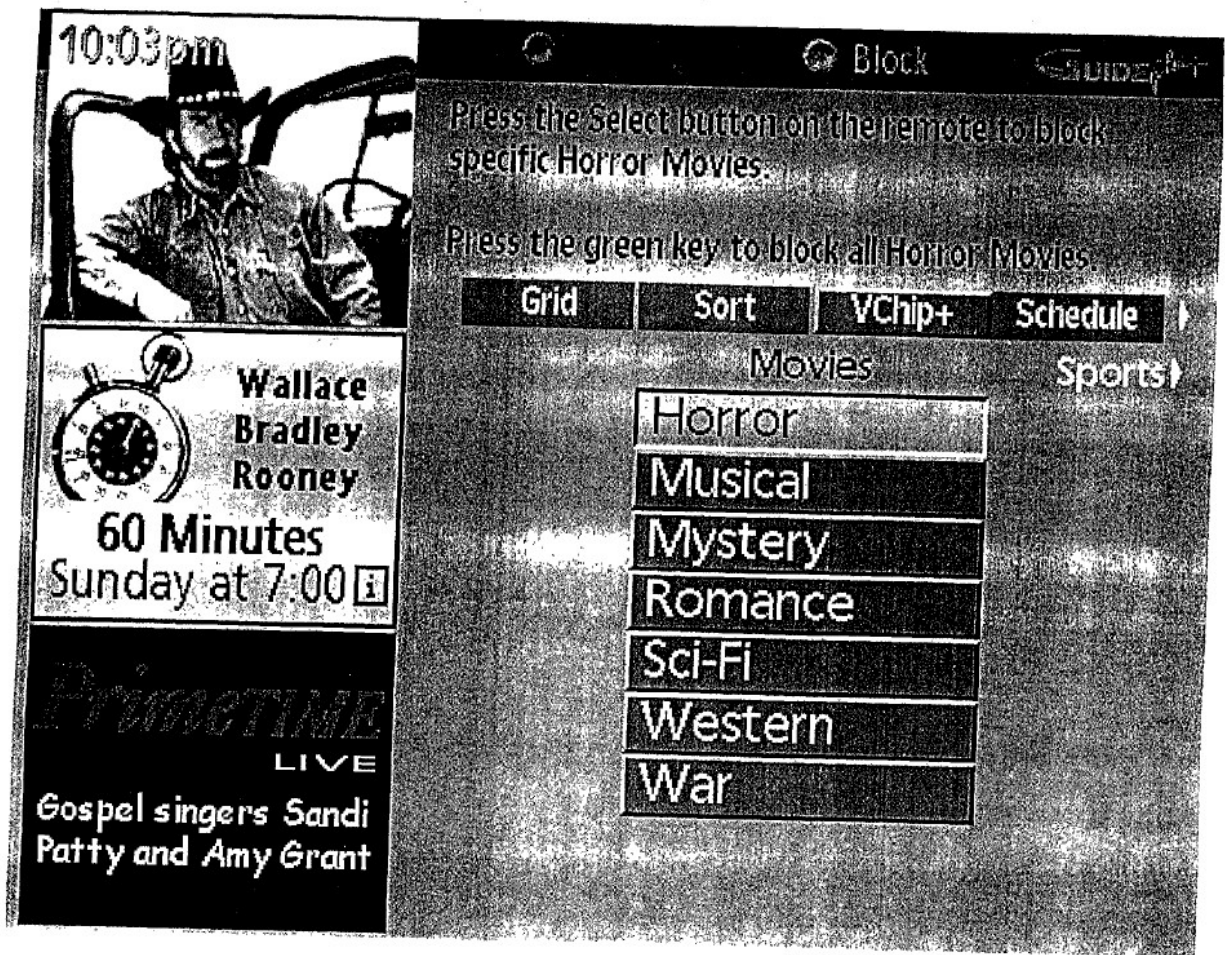


FIG 54

Leung, FIG. 54.

A POSITA would have been motivated to implement Leung’s genre-based locks in Sullivan’s PVR to increase a parent’s control over the content that their children watch by allowing a parent to block certain genres, regardless of the

content's rating. Houh ¶190. Sullivan discloses allowing a user to sort displayed content based on "category, e.g. Movies, Sports or Children's programs." Sullivan, [0175], FIG. 54. A POSITA would have found it obvious to implement Sullivan's PVR to likewise display and allow blocking of genres because Sullivan recognizes that parents may desire to control access to content based on "themes," e.g., "graphic violence or sexual themes." Houh ¶190; Sullivan, [0082], [0091]-[0092], FIG. 15. Because such genre-based control was well known, combining Sullivan and Leung to implement genre-based blocks would have been a combination of familiar elements according to known methods to predictably yield a desirable increase in access controls. Houh ¶190. A POSITA would have reasonably expected success because Leung teaches that this information was readily available in "a locally stored electronic program guide," and implementing it would have required only conventional adaptations of the same techniques used to block content based on other criteria (e.g., its theme and rating). Sullivan, [0073]-[0074], [0090]-[0092]; Leung, [0059], [0175]; Houh ¶190.

f. Claim 18: "The method of claim 12, wherein the media information comprises a media owner."

As discussed for [12d], Sullivan discloses "reading media information." As discussed for claim 9, Sullivan teaches, or it would have been obvious to implement based on Leung, a parental locks interface that allows blocking content

based on media information comprising a “media owner.” Houh ¶191. When implementing these media-owner blocks, Sullivan’s determining whether the content is blocked involves reading the content’s media owner to determine whether it violates a media-owner-based setting. Sullivan, [0073]; Houh ¶191. Because Sullivan’s “channel lock overlay” allows a user to block certain channels by name (e.g., media owner), a POSITA would have been motivated to maintain this block on content recorded by the parent onto the PVR from this media owner. Sullivan, [0038]; Houh ¶191. A POSITA would have reasonably expected success because this information was readily available, for example, in “a locally stored electronic program guide,” and implementing it would have required only conventional adaptations of the same techniques used to block content based on other criteria (e.g., its theme and rating). Sullivan, [0073]-[0074], [0090]-[0092]; Leung, [0059], [0175]; Houh ¶191.

- g. Claim 19: “The method of claim 12, further comprising retaining the associated authentication code of each user during a session associated with each user.”**

Sullivan and Craner render obvious the additional limitations of claim 19. Houh ¶¶192-195.

As discussed for [1g], Sullivan discloses authenticating a user’s authentication code. Houh ¶193. Similar to Sullivan, Craner discloses creating

parental control settings for “[e]ach user of the user equipment” and providing each user “a standard username and password combination” for authentication. Craner, 11:48-58; Houh ¶193. Craner discloses that the user equipment retains the associated password (authentication code) of each user during a session associated with each user. Craner, 11:48-65, 19:15-64, FIG. 14; Houh ¶193. Craner discloses that, when multiple users are defined, “users may be authenticated upon accessing or powering on the user equipment” or at “other convenient times” using their password. Craner, 11:48-65. Once authenticated, the system uses the parental control settings for “the current user” to determine whether that user “is authorized to access the asset.” Craner 19:52-64.

A POSITA would have been motivated to implement Craner’s ability to retain the most recent user’s authentication code and apply that user’s rating parameters when accessing additional content to avoid requiring the user to input their password each time they access content blocked for another user. Houh ¶194. Craner discloses that this feature was desirable because “users (e.g., children) may become frustrated over the frequent ... prompts for parental control access codes.” Craner, 1:34-36. By retaining that user’s password, users need only enter their password once per session to access all the content that complies with their profile. Houh ¶194. A POSITA would have reasonably expected success, given the similarity between Sullivan and Craner. Houh ¶195. Moreover, retaining a user’s

authentication code for a session would have required only conventional techniques. Houh ¶195.

VII. DISCRETIONARY DENIAL IS NOT WARRANTED

A. 35 U.S.C. § 314(a) Does Not Warrant Discretionary Denial

Patent Owner asserted the '879 patent against Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc. (collectively, "Samsung"), in the Eastern District of Texas. Ex. 1008. Under the factors in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 5-6 (Mar. 20, 2020) (precedential) ("*Fintiv*"), and the Office's interim guidelines dated June 21, 2022 ("Guidance Memo"), discretionary denial is not warranted.

Factor 6 requires institution because this Petition "presents a compelling unpatentability challenge." Guidance Memo at 4-5.

Factor 3 favors institution because Petitioners acted diligently and almost no parallel investment has occurred. Petitioners filed this Petition (and one challenging another asserted patent) roughly six months after Truesight served its infringement contentions. Ex. 1009; *see, e.g., Fintiv* at 11 ("[I]t is often reasonable for a petitioner to wait to file its petition until it learns which claims are being asserted against it in the parallel proceeding."); *CoolIT Sys., Inc. v. Asetek Danmark A/S*, IPR2021-01195, Paper 10 at 11-12 (PTAB Dec. 28, 2021) (finding diligence where petition was filed five months after infringement contentions were

served). The case is in early stages: the court has not yet engaged in claim construction, and discovery and dispositive motions will conclude after the Board's Institution Decision. Ex. 1010; *Protect Animals with Satellites v. OnPoint Sys., LLC*, IPR2021-01483, Paper 11 at 14-15 (PTAB Mar. 4, 2022).

Factor 1 is neutral because a stay has been neither requested nor granted.

Factors 2, 4, and 5 do not warrant denial. While trial is scheduled to begin October 6, 2025 (Ex. 1010) and Samsung is a defendant in the district court litigation, these factors are not determinative under *Fintiv* and must be weighed against Factors 3 and 6. *See, e.g., NetNut Ltd. v. Bright Data Ltd.*, IPR2021-01492, Paper 12 at 9-14 (PTAB Mar. 21, 2022). On balance, the *Fintiv* factors favor institution.

B. 35 U.S.C. § 325(d) Does Not Warrant Discretionary Denial

Discretionary denial under § 325(d) is not warranted. *See Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 7-11 (Feb. 13, 2020) (precedential) (“*Advanced Bionics*”).

Neither “the same or substantially the same art” nor “the same or substantially the same arguments” were previously presented to the USPTO. *Id.*, 8. Sullivan and Craner were never considered during prosecution. And the Examiner relied on Leung only to address deficiencies in a primary reference, Starikov (U.S. Patent Application Publication No. 2010/0287584). Ex. 1002, 120-121. The

USPTO has never evaluated the combination of Sullivan, Leung, and Craner presented in this Petition. Indeed, Sullivan teaches the only aspect of the claims the applicant argued was missing from Leung. *See id.*, 146-148 (arguing “Leung also does not teach or suggest overriding a given policy *on a per media basis, let alone a per authentication code (or a per user) basis* as recited”); *supra* [1a].

Had the Examiner known of Sullivan and Craner, it would not have allowed the claims of the ’879 patent to issue.

VIII. MANDATORY NOTICES

A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)

Google LLC, Samsung Electronics America, Inc., and Samsung Electronics Co., Ltd., are the real parties-in-interest for this Petition.³

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

To the best knowledge of Petitioners, the ’879 patent is or has been involved in the following district court litigations:

Name	Number	Court	Filed
<i>Truesight Commc’ns LLC v. Samsung Elecs. Co., Ltd. et al.</i>	2:23-cv-00643-JRG	E.D. Tex.	Dec. 29, 2023

³ 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.

<i>Truesight Commc'ns LLC v. TCL Tech. Grp. Corp.</i>	2:24-cv- 00032-JRG	E.D. Tex.	Jan. 22, 2024
<i>Truesight Commc'ns LLC v. Lenovo Grp. Ltd.</i>	2:24-cv- 00031-JRG	E.D. Tex.	Jan. 22, 2024

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Back-Up Counsel
Erika Harmon Arner (Reg. No. 57,540) erika.arners@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	Grace K. Mills (Reg. No. 66,946) gracie.mills@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Tel: 202-408-4000 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 Robert K. High (Reg. No. 75,786) robert.high@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 271 17th Street, NW Suite 1400 Atlanta, GA 30363-6209 Tel: 404-653-6400 Fax: 202-408-4400

	<p>Jeffrey A. Miller (Reg. No. 35,287) jeffrey.miller@apks.com Arnold & Porter Kaye Scholer LLP 5 Palo Alto Square, Suite 500 3000 El Camino Real Palo Alto, CA 94306 Tel: 650-319-4519 Fax: 650-319-4938</p> <p>Ali R. Sharifahmadian (Reg. No. 48,202) ali.sharifahmadian@arnoldporter.com Arnold & Porter Kaye Scholer LLP 601 Massachusetts Ave., NW Washington, DC 20001-3743 Tel: 202-942-5000 Fax: 202-942-5999</p>
--	--

In concurrently filed Powers of Attorney, Google LLC has granted Power of Attorney to Practitioners at Finnegan, Henderson, Farabow, Garrett & Dunner LLP, and Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. have granted Power of Attorney to Practitioners at Arnold & Porter Kaye Scholer LLP.

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Please address all correspondence to lead and back-up counsel at the addresses shown above and Google-Truesight-IPRs@finnegan.com. Petitioners also consent to electronic service by e-mail.

IX. GROUNDS FOR STANDING

Petitioners certify that the '879 patent is available for IPR and Petitioners are not barred or estopped from requesting IPR to challenge the claims on the grounds above. Petitioners filed this Petition within one year of service of the original complaint against Petitioners Samsung Electronics America, Inc., and Samsung Electronics Co., Ltd. in the district court litigation.

X. CONCLUSION

Petitioners request the Board institute IPR and cancel each challenged claim as unpatentable.

Date: December 27, 2024

Respectfully submitted,

/Erika H. Arner/

Erika H. Arner, Lead Counsel

Reg. No. 57,540

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing **Petition for *Inter Partes* Review** contains 13,997 words, excluding those portions identified in 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

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

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. §§ 42.6(e) and 42.105, the **Petition for *Inter Partes* Review of U.S. Patent No. 8,949,879, the associated Powers of Attorney, and Exhibits 1001-1018** were served via FedEx Priority Overnight on the correspondence address of record with the USPTO as follows:

Peter Lambrianakos
Fabricant LLP
411 Theodore Fremd Road
Suite 206 South
Rye, NY 10580

A courtesy copy has also been mailed to litigation counsel for Patent Owner at:

John Rubino
Rubino IP
51 J.F.K. Parkway
Short Hills, NJ 07078

Samuel Baxter
McKool Smith
300 Crescent Court
Suite 1200
Dallas, TX 75201

Dated: December 27, 2024

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