

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

**DECLARATION OF DR. HENRY HOUH,
UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITION FOR
INTER PARTES REVIEW**

TABLE OF CONTENTS

I.	Introduction.....	8
II.	Qualifications And Professional Experience.....	10
III.	Level Of Ordinary Skill In The Art.....	16
IV.	Relevant Legal Standards	17
V.	Technology Background.....	19
	A. Content Ratings	19
	B. The V-Chip.....	20
	C. User Profiles	21
VI.	Summary of the '879 Patent	22
	A. The Specification.....	22
	B. Prosecution History	26
VII.	Claim Construction.....	28
VIII.	Claims 1-19 Are Unpatentable	28
	A. Summary of the Prior Art.....	29
	1. Sullivan	29
	2. Leung.....	35
	3. Craner.....	37
	B. Ground 1: Claims 1-19 Are Obvious over Sullivan, Leung, and Craner	40
	1. Rationale for Combining Sullivan and Leung	40
	a. Combining Sullivan and Leung to implement a V-chip on Sullivan's PVR	41

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	45
2.	Independent Claim 1	52
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:”	52
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”	54
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,”	57
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,”	58
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,”	60
f.	[1e]: “wherein the first authentication code comprises a personal identification number (PIN),”	61

g.	[1f]: “wherein the different ratings associated with the specific digital content are enforced using the first and second authentication codes, and”	64
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.”	65
3.	Dependent Claims	67
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.”	67
b.	Claim 3: “The apparatus of claim 2, further comprising a data port for exporting the policy database to another playback device.”	68
4.	Independent Claim 4	70
a.	[4pre]: “A method in a computing system for creating specific rating policies for digital media access, the method comprising:”	70
b.	[4a]: “under control of the computing system having a memory and a processor, performing the acts of:”	71
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;”	72
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,” 75
e.	[4e]: “wherein the first viewer and second viewer are separate and distinct from the user from which the override actions are received, and” 80
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;” 80
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” 81
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,” 82
i.	[4i]: “wherein the first authentication code comprises a personal identification number (PIN), and” 83
j.	[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.” 83
5.	Dependent Claims 83
a.	Claim 5: “The method of claim 4 further comprising validating the authentication codes of the first viewer and the second viewer.” 83

b.	Claim 6: “The method of claim 4, wherein the first and second authentication codes comprise a personal identification number (PIN).”	84
c.	Claim 7: “The method of claim 5, wherein the authentication codes comprise biometric information.”	85
d.	Claim 8: “The method of claim 4, further comprising displaying the media information, wherein the media information comprises a media rating.”	86
e.	Claim 9: “The method of claim 4, further comprising displaying the media information, wherein the media information comprises a media owner.”	90
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.”	94
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.”	95
6.	Independent Claim 12	96
a.	[12pre]: “A method in a computing system for rating based media access policy enforcement, the method comprising:”	96
b.	[12a]: “under control of a video playback device having a V-chip that specifies default rating based access policy, performing the acts of:”	96
c.	[12b]: “displaying metadata;”	96

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:”	101
e.	[12d]: “reading media information”	103
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”	103
g.	[12f]: “responsive to determining that an authentication code is required: validating an authentication code; and”	104
	[12g]: “beginning playback of the media;”	104
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”	105
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,”	106
j.	[12j]: “wherein the first authentication code comprises a personal identification number (PIN), and”	107
k.	[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.”	107

7.	Dependent Claims	107
a.	Claim 13: “The method of claim 12, wherein the authentication codes comprise personal identification numbers.”	107
b.	Claim 14: “The method of claim 12, wherein the authentication codes comprise biometric information.”	108
c.	Claim 15: “The method of claim 12, wherein the default rating based access policy action is to deny access.”	108
d.	Claim 16: “The method of claim 12, wherein the media information comprises a rating.”	108
e.	Claim 17: “The method of claim 12, wherein the media information comprises a genre.”	108
f.	Claim 18: “The method of claim 12, wherein the media information comprises a media owner.”	111
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.”	112
IX.	Conclusion	113

I. Introduction

1. I make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters stated herein.

2. I have been asked by Google LLC, Samsung Electronics America, Inc., and Samsung Electronics Co., Ltd. (collectively, “Petitioners”) to provide my expert opinion connection with the *Inter Partes* Review of U.S. Patent No. 8,949,879 (“the ’879 patent”) to Zipperer et al. concerning whether the ’879 patent is unpatentable over certain prior art. This declaration is a statement of my opinions on issues relating to the patentability of claims 1-19 (“the Challenged Claims”) of the ’879 patent. As I explain more fully below, it is my opinion that all of the Challenged Claims would have been obvious to a person of ordinary skill in the art (“POSITA”) at the time of the alleged invention.

3. I am being compensated for my work in this matter at my standard hourly rate. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this investigation. My compensation is not contingent on the outcome of this matter or the specifics of my testimony.

4. I have reviewed and considered the following documents in connection with my analysis of the ’879 patent:

Exhibit	Description
Ex. 1001	U.S. Patent No. 8,949,879 to Zipperer et al. (“the ’879 patent”)

Exhibit	Description
Ex. 1002	File History of U.S. Patent No. 8,949,879
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. 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”)

5. In forming the opinions expressed below, I have considered:

- a) the documents listed above;
- b) the relevant legal standards, including the standard for obviousness, and any additional authoritative documents as cited in the body of this declaration; and

c) my own knowledge and experience based upon my work in the field of software systems as described below, as well as the following materials.

6. Unless otherwise noted, all emphasis in any quoted material has been added.

II. Qualifications And Professional Experience

7. My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Exhibit 1004. The following is a brief summary of my relevant qualifications and professional experience.

8. I received a Ph.D. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (“MIT”) in 1998. Beforehand, I received a Master of Science degree in Electrical Engineering and Computer Science in 1991, a Bachelor of Science degree in Electrical Engineering and Computer Science in 1989, and a Bachelor of Science degree in Physics in 1990, all from MIT.

9. I am currently self-employed as an independent technical consultant. From its founding in 2012 until October 2022, I was also president of a company that provides supplemental science, technology, engineering, and mathematics (“STEM”) education to children of all ages.

10. I first entered telecommunications in 1987 when I worked as a summer intern at AT&T Bell Laboratories as part of a five-year dual degree program at MIT. I continued to work at AT&T Bell Laboratories as part of this MIT program. While at MIT, I was a teaching assistant (“TA”) in the Electrical Engineering and Computer Science Department’s core Computer Architectures course. I first was a TA as a senior for a role typically reserved for graduate students. I later became head TA. The course covered various topics in computer architectures. As a TA, I helped write homework assignments, lab assignments, and exams. I also taught in the recitation sections.

11. Later, as part of my doctoral research at MIT from 1991-1998, I was a research assistant in the Telemedia Network Systems (“TNS”) group at the Laboratory for Computer Science. The TNS group built a high-speed gigabit network and created applications that ran over the network. Example applications included ones for remote video capture, processing, and display of video on computer terminals. In addition to working on the design of core network components, designing and building the high-speed links, and designing and writing the device drivers for the interface cards, I also set up the group’s web server. Also, I helped to maintain, install, and upgrade the networking devices used within the group, along with other graduate students. When I started with the TNS group, the networking infrastructure consisted of shared coaxial cable-based

Ethernet, with bridges and repeaters interconnecting various network segments.

We gradually replaced the coaxial Ethernet infrastructure with twisted pair

10BASE-T wiring that were interconnect via hub repeaters, for which we also had to mind the Ethernet specifications. Eventually, many of the hub repeaters were upgraded to switches. I also studied the various parts of the Ethernet specifications both independently and through graduate course work in networking.

12. I also helped to build the web pages that initiated the above-mentioned video sessions via a web interface. Vice President Al Gore visited our group in 1996 and received a demonstration of—and remotely drove—a radio-controlled toy car with a wireless video camera mounted on it that was built by our group. This toy car device received commands transmitted over a network from a remote computer, and video data from the toy car was transmitted wirelessly then over a computer network back to the user controller. On occasion, we allowed users visiting our web site to drive the toy car from their remote computer while they watched the video on their computer. The video stream was encoded by TNS-designed hardware, streamed over the TNS-designed network, and displayed using TNS-designed software.

13. I defended and submitted my Ph.D. thesis, titled “Designing Networks for Tomorrow’s Traffic,” in January 1998. As part of my thesis research, I analyzed local area and wide area flows to show a more efficient method for

routing packets in a network, based on traffic patterns at the time. The traffic flow data included Ethernet, IP, TCP or UDP, and RTP header information, which I analyzed to come to the conclusions in my thesis.

14. While I was in graduate school, I started a company that provided web site design services and targeted advertising opportunities. We also sold targeted advertising placements. As the web became popular first at colleges and universities, we focused initially on building college recruiting web sites and sold advertisements to companies wishing to target students to recruit at specific colleges. We developed technology that utilized the web user's college affiliation to customize advertisements targeted to students at that college.

15. From 1997 to 1999, I was a Senior Scientist and Engineer at NBX Corporation, a start-up that made business telephone systems for streaming packetized audio over data networks instead of using traditional telephone lines. NBX was later acquired by 3Com Corporation and the phone system is still used today by numerous businesses.

16. As part of my work at NBX, I designed the core audio reconstruction algorithms for the telephones, as well as the packet transmission algorithms. I also designed and validated the core packet transport protocol used by the phone system. The protocol was used for all signaling in the phone system, including for the setup of conference calls. The NBX system also featured a computer interface

for initiating phone calls, which could also initiate conference calls. The NBX system also supported the Telephony Application Programming Interface (“TAPI”) that allowed other computer programs to integrate with our system telephony features. We obtained U.S. Patent No. 6,967,963, entitled “Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data,” as part of this work. The first release of the phones worked using Ethernet-layer packets (without the use of IP). I also programmed the first prototype of our phone which communicated using IP, and I demonstrated our IP phones working over the Internet when we attended a trade show in California. The phone connected over the Internet to our headquarters in Andover, MA.

17. From 1999-2004, I was employed by Empirix or its predecessor company, Teradyne. Teradyne had traditionally made products to test chips and hardware, but the founder and board chairman, Alex d’Arbeloff wanted to expand the company’s products to include software systems testing. Teradyne made a number of acquisitions to achieve this goal, and I was hired to work for Mr. d’Arbeloff to work with all the acquired software test divisions. These divisions were later spun-out of Teradyne into a separate company, Empirix. Empirix was a leader in test tools for software systems including telecommunications protocols and systems, providing functional testing tools as well as load testing tools. From 2000-2001, I conceived and built a test platform for testing Voice-over-IP (VoIP).

The first application on this new test platform was a cloud emulator for simulating the effects of transmitting VoIP over a busy network. The test platform was based on a network processor chip, which could be programmed to cut-through packets while processing packet data such as various protocol layer headers including addresses included therein and even packet data contents. I also designed a protocol analyzer built on the same platform. The application captured and performed protocol decoding at various layers in the protocol stacks of captured packets, including detailed Ethernet header decoding, IP header decoding, TCP header decoding, UDP header decoding, RTP header decoding, and many other specified protocols. The application was also designed to reconstruct entire conversations that spanned multiple packets.

18. In 2006, as part of my role at BBN Technologies, I helped found PodZinger Inc., now known as RAMP Inc. PodZinger utilized BBN's speech recognition algorithms to search through the spoken words in audio and video segments. While I was Vice President of Operations and Technology, PodZinger followed its initial prototype with a full streaming audio and video search solution. Our video and audio search results were integrated with a specialized player that incorporated metadata into the video player so that metadata could be used to select the exact portion of the video which to play. I also created a social networking web site, which BBN sold to a venture-funded startup company. In the

process of creating the web site, I designed and specified the authentication and authorization protocols.

III. Level Of Ordinary Skill In The Art

19. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

20. I understand that the '879 patent was filed on April 19, 2012, and claims priority to U.S. Provisional Patent Application No. 61/478,204 filed on April 22, 2011. My analysis reflects the views of a person of ordinary skill in the art ("POSITA") in the field of the '879 patent as of April 22, 2011. That person 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. I was a person of ordinary skill in the art as of April 22, 2011.

21. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my experience and the understanding of a POSITA generally (and specifically related to the references I

consult herein), reflect the knowledge that existed in the field as of the earliest claimed priority date of the '879 patent (i.e., April 22, 2011). Unless otherwise stated, when I provide my understanding and analysis below, it is consistent with the level of a POSITA prior to the earliest claimed priority date of the '879 patent.

IV. Relevant Legal Standards

22. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the '879 patent, I am relying on certain basic legal principles that counsel have explained to me. These principles are discussed below.

23. I understand that prior art to the '879 patent includes patents and printed publications in the relevant art that predate the proper priority date of the alleged invention recited in the '879 patent.

24. I have been informed that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. I have also been informed by counsel that the obviousness analysis takes into account factual inquiries including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

25. I have been informed by counsel that the Supreme Court has recognized several rationales for combining references or modifying a reference to show obviousness of claimed subject matter. Some of these rationales include the following: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

26. I further understand that certain factors may support or rebut the obviousness of a claim. I understand that such secondary considerations include, among other things, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected results of the invention, any long-felt but unsolved need in the art that was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art, and copying of the

alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention. I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness.

27. I am not aware of any allegations by the named inventors of the '879 patent or any assignee of the '879 patent that any secondary considerations are relevant to the obviousness analysis of any Challenged Claim of the '879 patent.

V. Technology Background

A. Content Ratings

28. Most people are familiar with the MPAA (Motion Picture Association of America) film rating system, with ratings from G (General Audience), PG (Parental Guidance), PG-13 (Parents Strongly Cautioned), R (Restricted) to NC-17 (No One 17 or Under Admitted). These ratings help guide viewers about the content and appropriateness of films for different audiences.

29. Similarly, for television shows, V-Chip rating levels help parents monitor and control the content their children watch on television. Ratings indications include TV-Y (All Children), TV-Y7 (Older Children), TV-Y7-FV (Older Children, Fantasy Violence), TV-G (General Audience), TV-PG (Parental Guidance), TV-14 (Parents Strongly Cautioned), and TV-MA (Mature Audiences).

30. These ratings are intended to give information about a movie or television show that may be used by parents to help them decide whether the programming is appropriate for their children. While enforcement of movie ratings for movie patrons requires human intervention, the V-Chip ratings enforcement can be done automatically.

B. The V-Chip

31. As the '879 patent acknowledges, televisions in the U.S. have, by law, included “V-chip technology” since 2000 “to provide parents control over the programs that their children watch on television through broadcast, cable, or satellite television.” Ex. 1001, 1:19-25. Televisions with a V-Chip may be programmed to automatically block television content based on the rating of a television program and the rating levels allowed to be viewed, as programmed into the television. “The V-chip uses the program rating” that is “contained within the television broadcast” and a “rating policy configuration to determine if the program is allowed or blocked.” Ex. 1001, 1:25-28, 1:58-60. If blocked, “a parent may input a PIN code allowing the program to be viewed without changing the policy configuration.” Ex. 1001, 1:60-63. This mechanism provides an automated method to block programs deemed not acceptable to view.

32. The rating of a television program is encoded in the vertical blanking interval of a television frame, in the same area where closed caption information is

transmitted. Leung, [0003]. The V-Chip decodes this information to determine the rating of the current program, and uses this information to decide whether the current settings allow for display of the program, or whether the program should be blocked.

C. User Profiles

33. User profiles are a concept that dates back to early days of media distribution, as content providers have long sought to understand and segment their audiences, and long segmented and categorized the users. However, while it was possible to segment users in the aggregate, media providers could not easily receiving information on individual viewers. Early in the digital age, user profiles were used distinguish between different users on a single computer, and track users individually and distinguish between different accounts, based on login credentials. In the early 1970's, the UNIX operating system included user profiles for accounts that captured user's names, phone numbers, office, as well as different groups the users belonged to, in order to determine which information on the computer the user was able to access.

34. With the advent of the world-wide web, the introduction of "cookies" in 1994 allowed the tracking of state during browser sessions, and was soon thereafter used to target content, such as advertising, to users. Cookies could be used to track a user's activity as well as capture their content preferences and

interests, so that appropriate ads could be shown to the user.

VI. Summary of the '879 Patent

A. The Specification

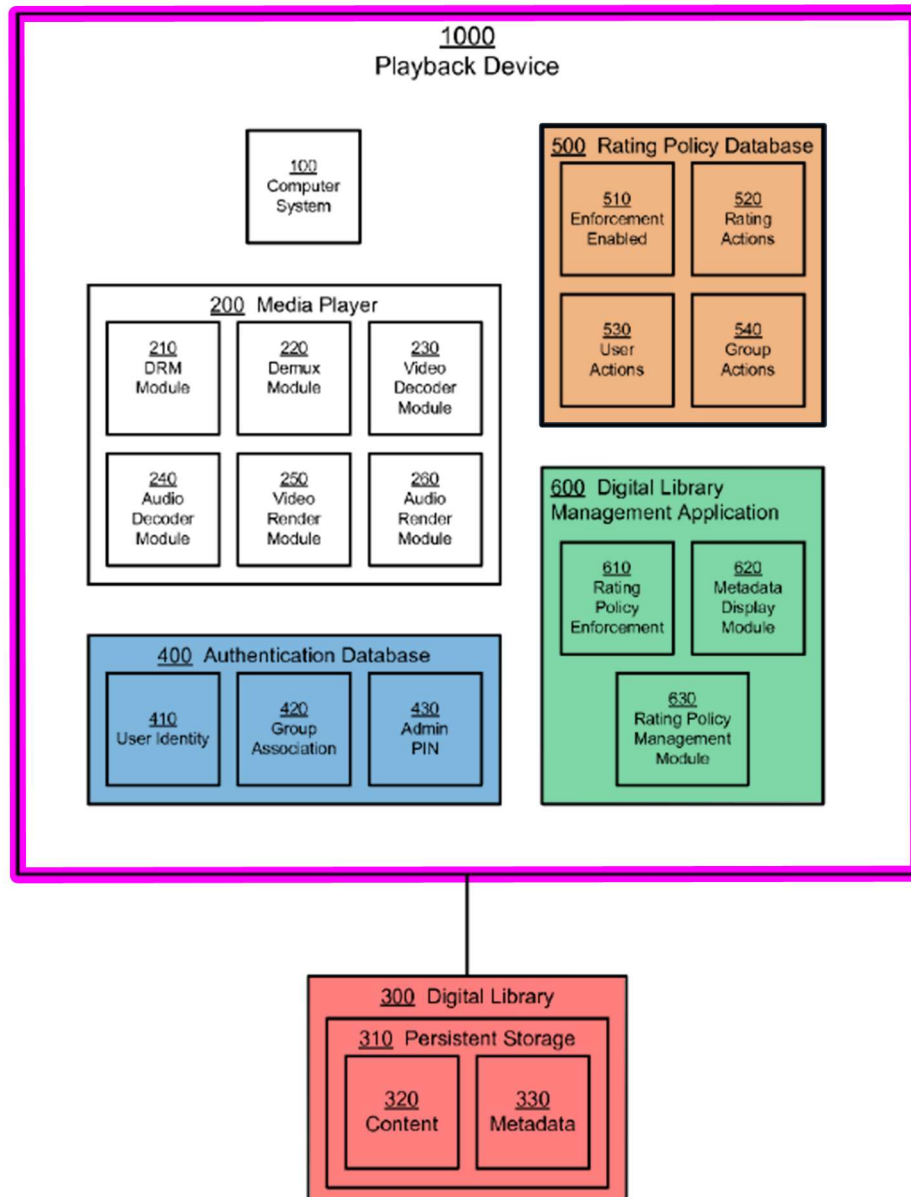
35. The '879 patent purports to overcome problems with the V-chip. For example, the '879 patent describes imposing content restrictions on a per user basis, allowing a parent to set different levels of access for multiple individual children (as opposed to restrictions that apply equally to all unauthorized users of a system). Additionally, the '879 patent describes imposing content restrictions on a per media basis, allowing a parent to set content restrictions for a particular program (as opposed to all programs with a certain rating).

36. In particular, the '879 patent relates to access controls for content on video playback devices that “play content from a digital library stored either locally or remotely.” Ex. 1001, Title, 1:13-15. The '879 patent states that a digital library, which allows consumers to watch a “program multiple times at their convenience, outside of a scheduled broadcast,” “typically contains content for a single household, not a single individual.” Ex. 1001, 2:9-20, 2:33-34. According to the '879 patent, “the single override” using the PIN that is conventionally “available using V-chip technology is insufficient” in households with children of different ages because “the most restrictive rating policy must be implemented.” Ex. 1001, 2:33-48. The '879 patent also states that the program rating “may not

coincide with the parent's judgments." Ex. 1001, 2:49-60.

37. The '879 patent describes "a computing configuration for use with digital library ratings enforcement" that allows multiple user authenticators and parental overrides of a program rating. Ex. 1001, 3:1-2, 6:1-7:21. Figure 2, below, depicts an example "computing configuration for use with a digital library."

Ex. 1001, 5:5-6.

**FIG. 2**

Ex. 1001, FIG. 2 (annotated).

38. The computing environment includes a digital library 300, authentication database 400, rating policy database 500, and digital library management application 600. Ex. 1001, 5:6-10, FIG. 2. The digital library 300

stores content 320 and associated metadata 330 and is either coupled to or contained within a **playback device 1000**. Ex. 1001, 5:6-10, 5:29-67. The **authentication database 400** includes user identity 410, which “contains user authenticators”; group associations 420, which “contain sets of users”; and administration PIN 430. Ex. 1001, 6:1-54.

39. “The **rating policy database 500** stores content rating override actions and metadata display actions configured by the parent.” Ex. 1001, 6:55-57. For example, both user actions 530 and group actions 540 are “content playback actions where the stored rating is different than was set by the rating body” and include “mappings between the user identifier, content identifiers, content rating system, and new content rating.” Ex. 1001, 7:3-21.

40. The **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 the **authentication database 400** and the **rating policy database 500** to determine if the user is able to watch the content.” Ex. 1001, 7:30-44, 8:58-9:10. Figure 5, below, depicts the process “for determining if a PIN is required using multiple policies.” Ex. 1001, 9:23-10:3, FIG. 5. The **digital library management application 600** also includes a rating policy management module 630 that “allows

the user to modify (e.g., create, update, and/or delete) data stored in the **digital library 300**, **authentication database 400**, and **rating policy database 500**.”

Ex. 1001, 7:30-33, 7:55-58.

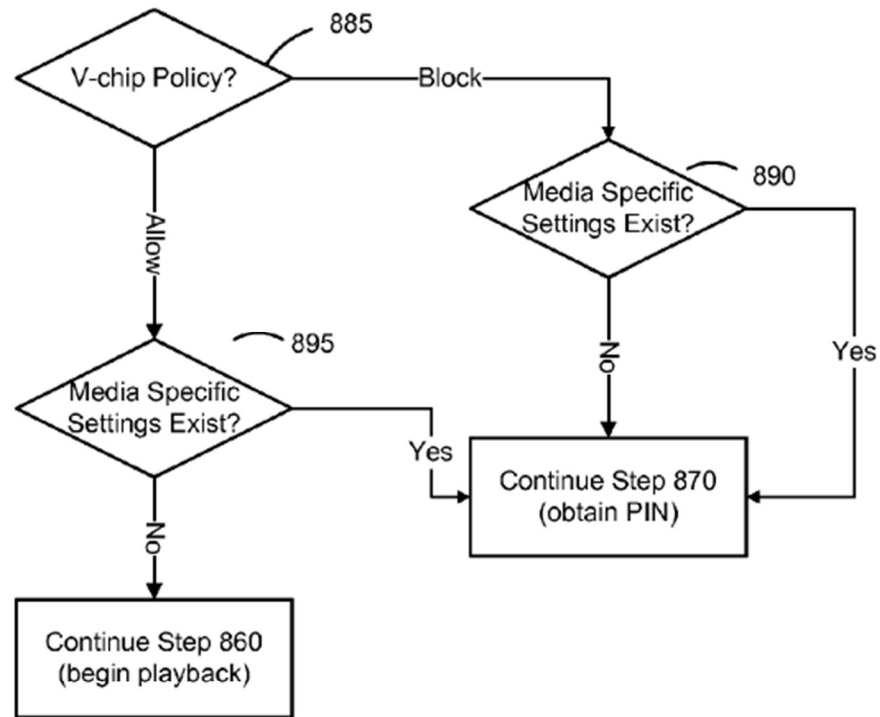


FIG. 5

Ex. 1001, FIG. 5.

B. Prosecution History

The '879 patent was filed as U.S. Patent Application No. 13/451,510 on December 13, 2012. Ex. 1001 at Cover. The Examiner initially rejected the claims as either anticipated or rendered obvious. Ex. 1002, 72-77. Applicant then

amended the claims “to clarify that the access controls referred to in the claims are rating based access controls used (*e.g.*, by parents) to override rating policies set by V-chips for the media industry.” Ex. 1002, 90-93. Applicant argued that the cited prior art’s disclosure of digital rights management differed from the claimed access controls. Ex. 1002, 94-96.

The Examiner again rejected the claims as anticipated or rendered obvious. Ex. 1002, 117-124. Applicant then amended the claims “to clarify that the rating based access control policy allows overrides that are different for at least two different users that are separate and distinct from the administrator (or master user that sets up the system).” Ex. 1002, 141-145. Applicant argued that the cited references did not teach “at least two different users (apart and separate from the administrator or master of the system) having different responsive authentication codes that are used to allow or deny access to media *on a per media basis on a per user* (or group of users) *basis* in order to override a V-chip rating system.” Ex. 1002, 146-148. Applicant argued that “this allows a parent, for example, to override a V-chip differently for different aged children with respect to a particular piece of content so that the youngest child’s needs are not forced to determine the override policy.” Ex. 1002, 146.

The Examiner then issued a notice of allowance with an examiner’s amendment. Ex. 1002, 164-168. The amendment added to claim 1 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” and added a similar limitation to the other independent claims. Ex. 1002, 165-168.

VII. Claim Construction

41. It is my understanding that in order to properly evaluate the ’879 patent, the terms of the claims must first be interpreted. It is my understanding that for the purposes of this inter partes review, the claims are to be construed under the so-called Phillips standard, under which claim terms are given their ordinary and customary meaning as would have been understood by one of ordinary skill in the art in light of the specification and prosecution history, unless the inventor has set forth a special meaning for a term. For the purposes of this declaration, it is my opinion that none of the claim terms requires a specific construction

VIII. Claims 1-19 Are Unpatentable

42. I have been asked to provide my opinion as to whether the Challenged Claims of the ’879 patent would have been obvious in view of the prior art. The discussion below provides a detailed analysis of how the prior art references identified below teach the limitations of the Challenged Claims of the ’879 patent.

43. As part of my analysis, I have considered the scope and content of the

prior art and any differences between the alleged invention and the prior art. I describe in detail below the scope and content of the prior art, as well as any differences between the alleged invention and the prior art, on an element-by-element basis for each Challenged Claims of the '879 patent.

44. As described in detail below, the alleged invention of the Challenged Claims would have been obvious in view of the teachings of the identified prior art references as well as the knowledge of a POSITA.

Ground	Claims	Basis	Prior Art
1	1-19	§ 103	Sullivan, Leung, and Craner

A. Summary of the Prior Art

45. In my opinion, Sullivan, Leung, and Craner are all analogous art to the '879 patent because each is from the same field of endeavor, providing personalized access controls for associated content, and is reasonably pertinent to one of the problems dealt with in the '879 patent, such as overriding default rating based controls. Ex. 1001, Abstract, 2:49-60; Sullivan, Abstract, [0006]-[0007], [0088]-0092], [0095]-[0101]; Leung, Abstract, [0004]-[0005], [0052]-[0057]; Craner, Abstract, 9:3-10:60, 11:36-12:59.

1. Sullivan

46. I have been informed that Sullivan, which was filed June 24, 2004, and published February 3, 2005, qualifies as prior art to the '879 patent.

47. Like the '879 patent, Sullivan discloses “[a] content control system for limiting access by sensitive users, such as children, or the like, to certain types of content.” Sullivan, Abstract. Sullivan recognizes that televisions included “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]. Sullivan also 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].

48. Sullivan provides a system with “simplified control of parental lock settings” and that “allows a user to modify the content rating of media recorded by a content recorder as the user sees fit.” Sullivan, [0007]. The system discloses 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.” Sullivan, [0009].

49. One such audiovisual device is “a content recorder,” such as a

personal video recorder (“PVR”). Sullivan, [0095]. The content recorder includes “a hard disk drive” and “is used to receive and display television content, such as from a television receiver or the like.” Sullivan, [0096]. The content recorder “prevent[s] unauthorized users from viewing restricted content” stored in the storage medium based on the rating of the stored content, a user’s rating lock level, and an exception list. Sullivan, [0088]-[0089], [0095]-[0101].

50. Sullivan discloses a “parental locks interface” such as the “content rating lock display screen 222” depicted below. Sullivan, Abstract, [0002], [0037], [0039]. In this screen, the “user may select particular ratings to lock and unlock” and then press the “Turn On Parental Locks” button 244 “to turn on parental locks after a user’s selections have been made by mapping a user’s selections to” the native parent control subsystem of each device in the computer system, including the content recorder. Sullivan, Abstract, [0039]-[0040], [0044], FIG. 4. “In the simplest embodiment, where a user selects a particular rating, that rating and all higher ratings will be locked.” Sullivan, [0053].

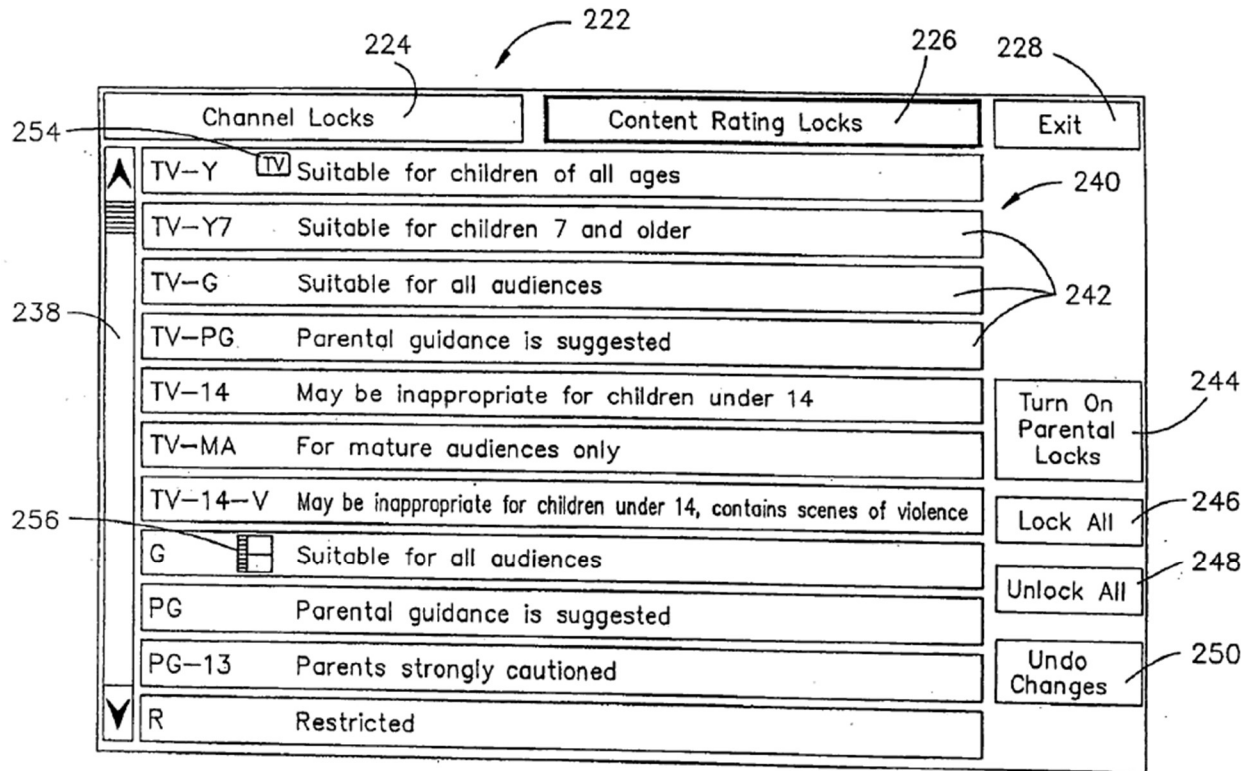


FIG. 4

Sullivan, FIG. 4.

51. “Where there are children of different ages, separate 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]. “Thus, a young child may have more restrictive acceptable content rating parameters than would a teenaged child, who may, in turn, have more restrictive acceptable content rating parameters than would an adult.” Sullivan, [0088].

52. Sullivan discloses that the content recorder’s content control system allows a user to “alter a rating associated with the received television content”

when the user believes that the “content rating for content the user has viewed” is not “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]-[0007], [0096]. Sullivan also discloses that the PVR includes “a unique password for a user or a group of users,” where, for example, “a seven year old child may have one password” and “a thirteen year old may have another password.” Sullivan, [0099]. An authorized user (e.g., a parent) adds another user (e.g., the thirteen year old) to “an exception list associated with” specific content stored in the PVR “denoting at least one user who is allowed to access the content and who would otherwise be blocked by application of the [original] content rating.” Sullivan, [0099]-[0100]. This process is depicted in Figure 17, below.

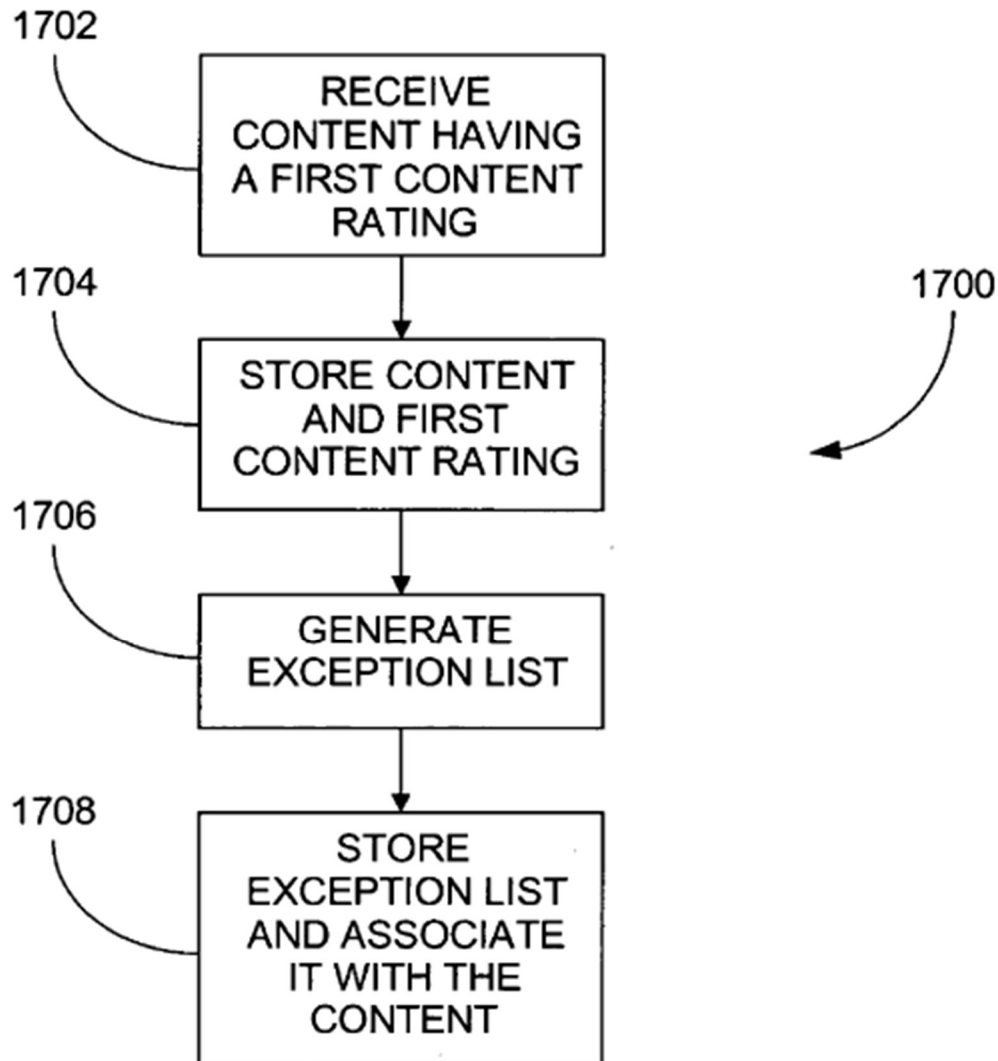


FIG. 17

Sullivan, FIG. 17.

53. If content is restricted, Sullivan's content control system allows authorized users to access the content by entering the password associated with their profile. Sullivan, [0074], [0077], [0089]-[0090], [0099].

2. Leung

54. I have been informed that Leung, which was filed October 16, 2001, and published July 18, 2002, qualifies as prior art to the '879 patent.

55. Leung discloses “exercising access control over television programs using a parental control user interface.” Leung, Abstract. Leung discloses that the V-chip system allows “a consumer to program his or her television system to exclude programs according to their preferred levels of one or more” rating criteria or “to permit only programs having certain levels of content according to these rating categories.” Leung, [0003]. Leung recognized that the V-chip’s effectiveness “depends on whether the consumer agrees with the subjective ratings contained in the VBI for most, if not all, programs.” Leung, [0004]. Regardless of how the ratings are made, many “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].

56. To address this issue, 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]. Leung provides “functionality which allows the two systems to work together to form a system which is an improvement over either system.” Leung, [0052]. “[T]he user is allowed to override the operation of the V-Chip system for particular programs

contained in user programmable enable override lists and blocking override lists.”

Leung, [0052]. Figure 1, below, depicts “the operation of this override system.”

Leung, [0053].

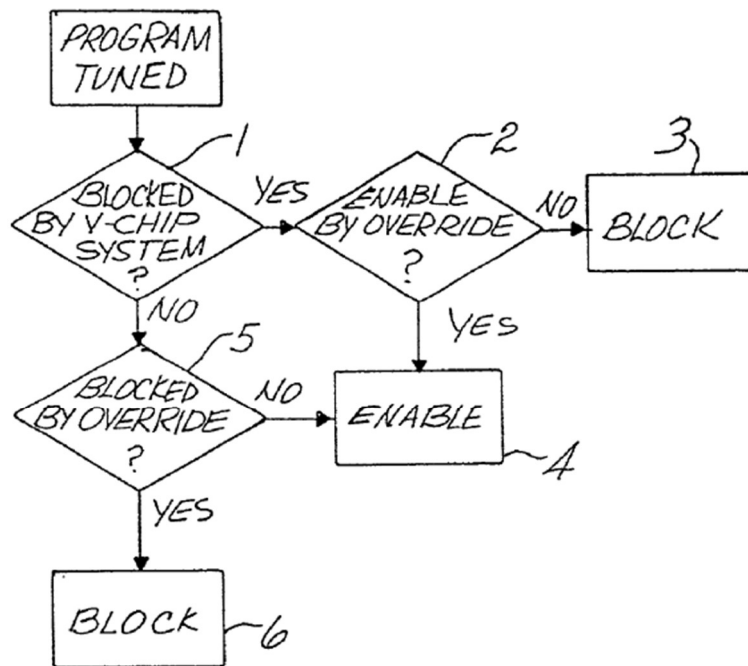


Fig. 1

Leung, FIG. 1.

57. In this combined system, “the user programs the television system to exclude programs according to one or more” rating criteria. Leung, [0065]. The system stores the user selections in internal memory and compares them with the rating factor transmitted in the VBI. Leung, [0065]. If an excluded program is detected, the program is blocked unless it appears on “an enable override list.” Leung, [0065]. Conversely, if a program “is not excluded under the rating criteria

established by the user,” it is allowed unless it appears on “a blocking override list.” Leung, [0065].

58. 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 “3 to 7 digit number” 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].

3. Craner

59. I have been informed that Craner, which was filed April 10, 2006, and issued December 13, 2011, qualifies as prior art to the ’879 patent.

60. Craner discloses a parental control system implemented on user equipment “suitable for providing interactive media functionality,” including a television or 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.

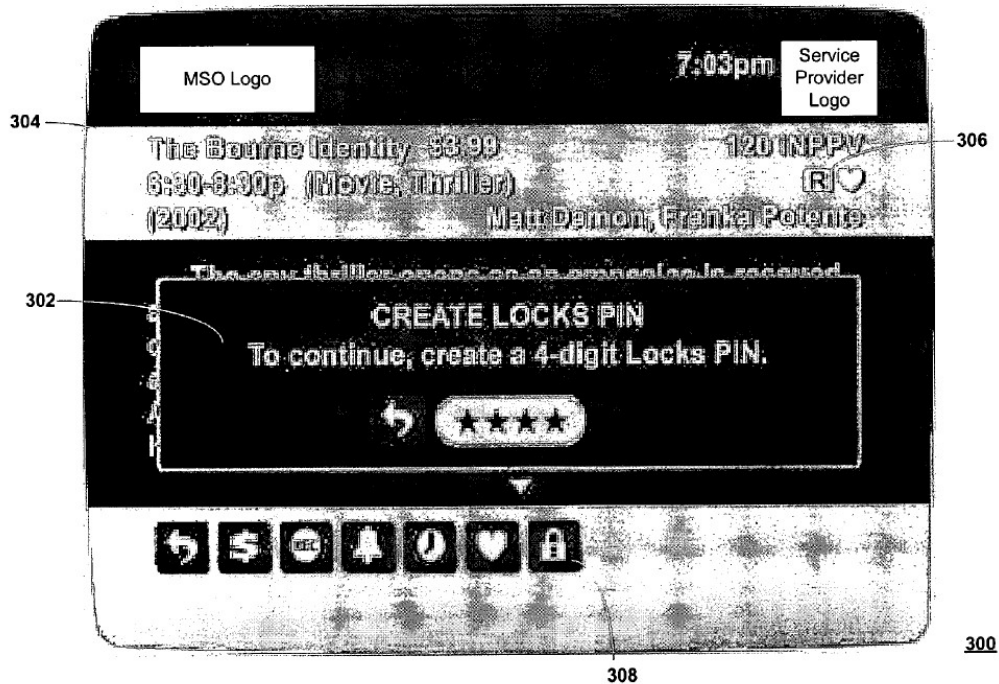


FIG. 3

Craner, FIG. 3.

61. 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. The customized settings for each user include “[t]itle locks” that “restrict access to content by title” and “ratings locks” that lock television programs and movies by rating. Craner, 12:7-43. Figure 6, below, depicts a “locks setup display screen 600” for one user. Craner, 11:48-50.

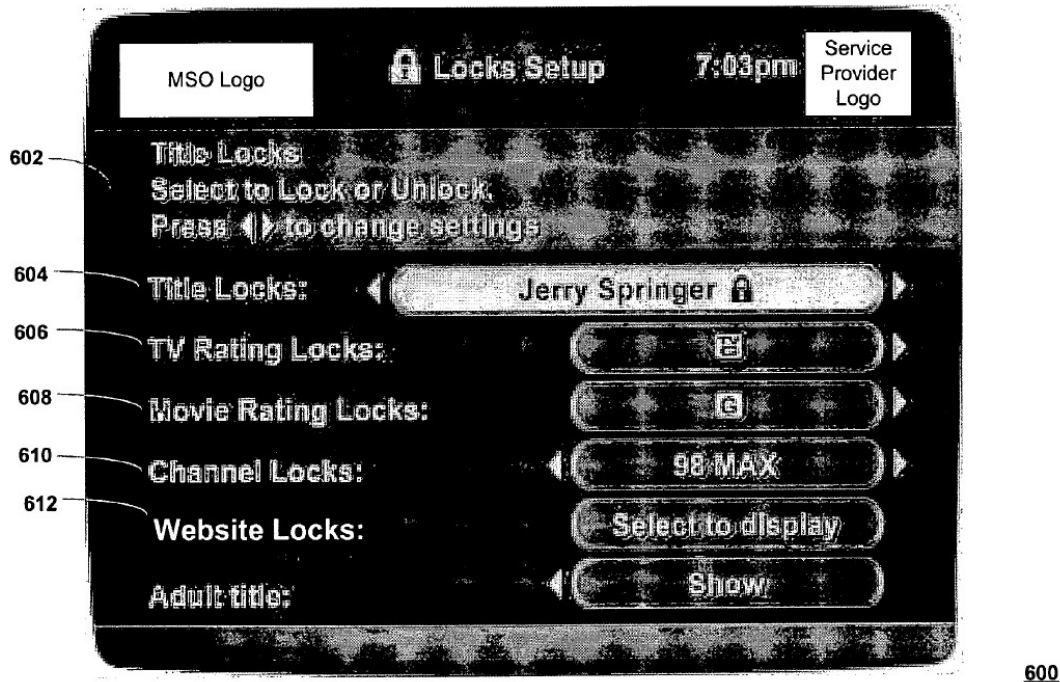


FIG. 6

Craner, FIG. 6.

62. 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 be given a parental control access code so that it can 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.

63. 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.

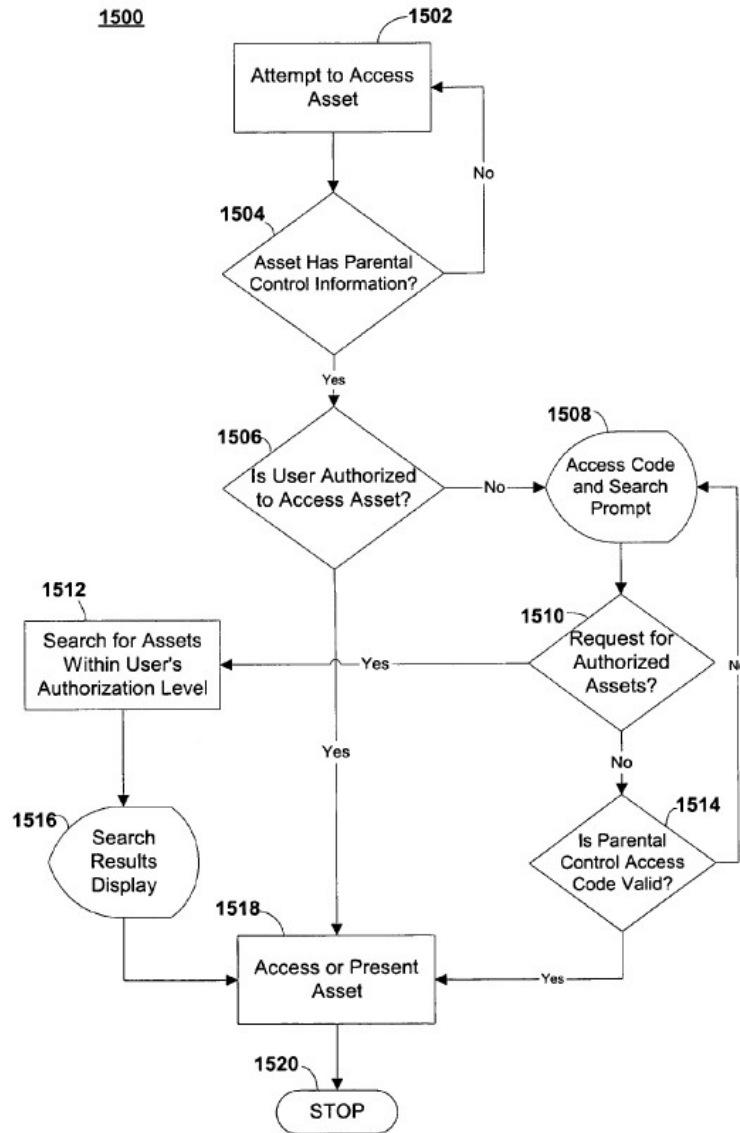


FIG. 15

Craner, FIG. 15.

B. Ground 1: Claims 1-19 Are Obvious over Sullivan, Leung, and Craner

1. Rationale for Combining Sullivan and Leung

64. In my opinion, 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 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

65. Sullivan discloses content recorders and other information appliances, such as PVRs, that 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 also discloses “a user interface for an ... information appliance, content recorder, or the like that provides 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 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]. An example interface is depicted in Figure 4, below. 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.

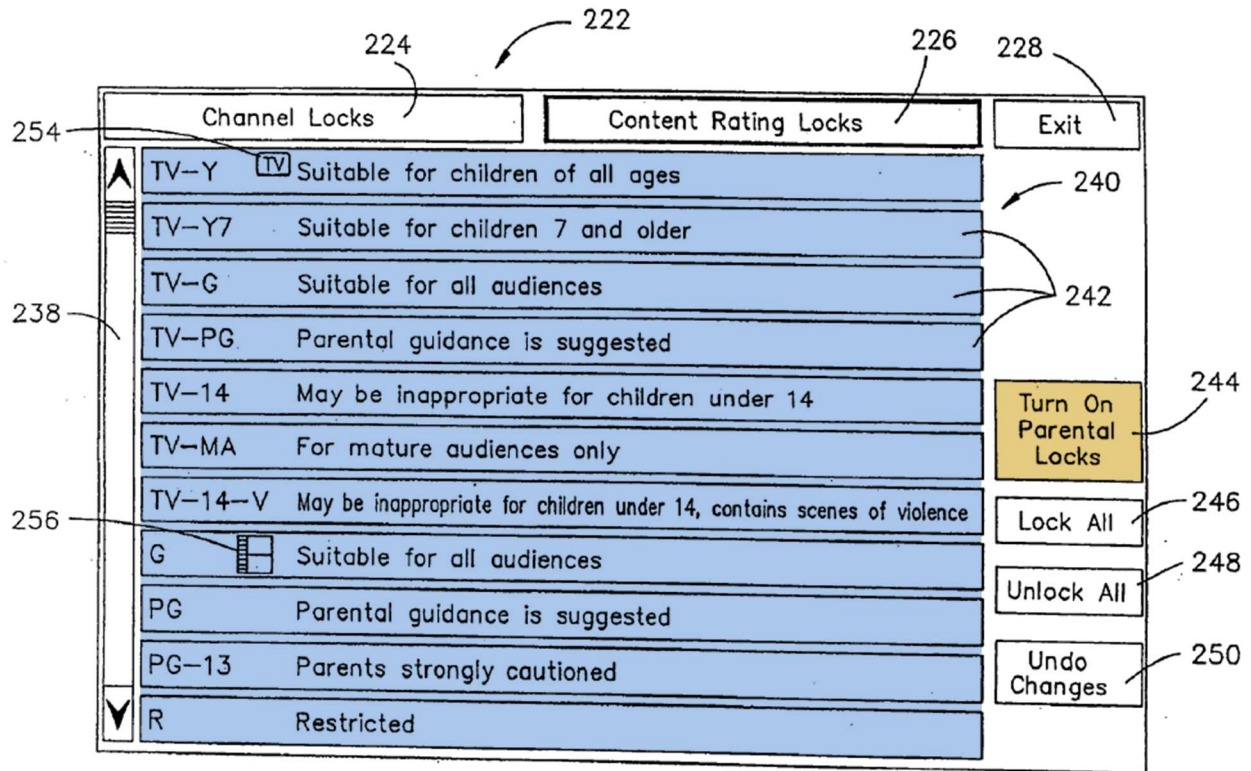


FIG. 4

Sullivan, FIG. 4 (annotated).

66. While Sullivan does not expressly disclose a V-chip, a POSITA would have found it obvious to combine Sullivan and Leung to implement Sullivan's ratings-based parental locks on Sullivan's PVR using a V-chip within the PVR's native parental control subsystem. A V-chip, depicted below, allows parents "to program his or her 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].

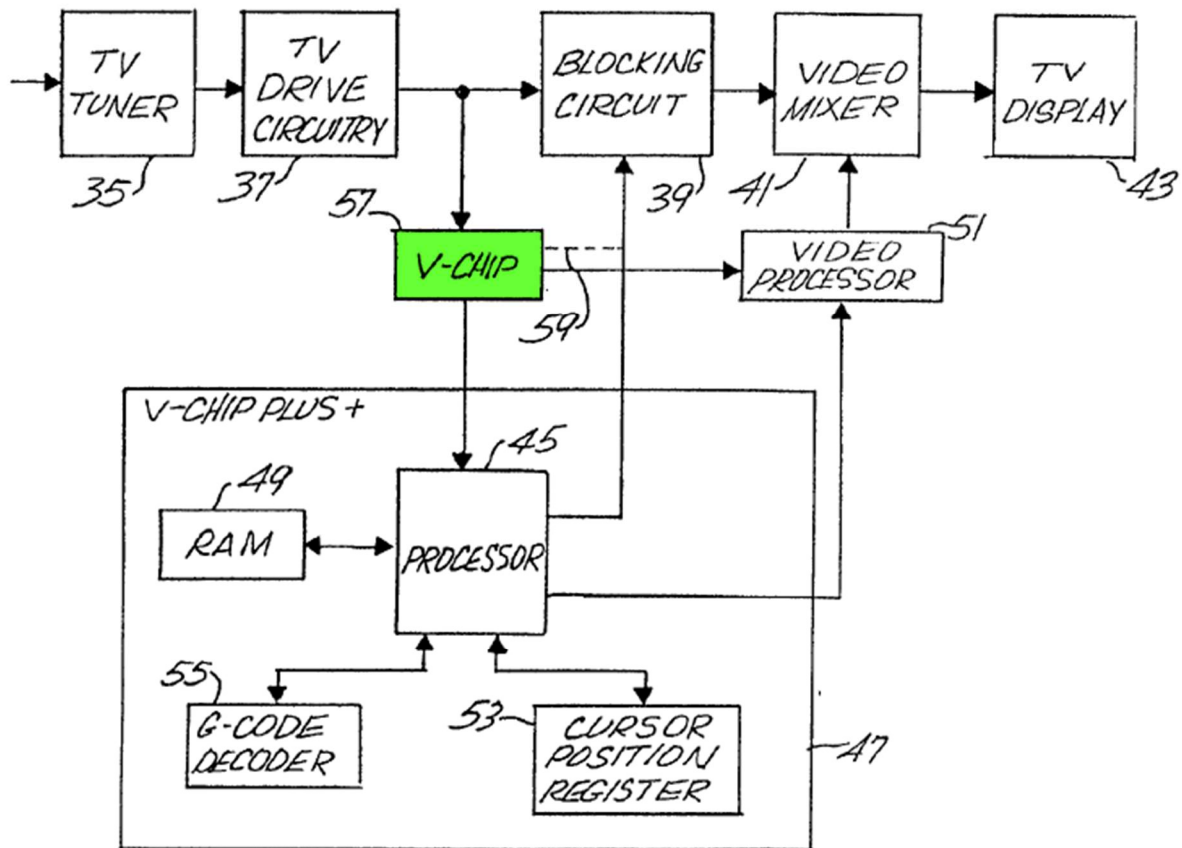


Fig. 5

Leung, FIG. 5 (annotated).

67. 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. 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 (“[T]he so-called v-chip technology provides a decoder to decode program rating data encoded into a program at the time it is broadcast and to selectively pass or block television programming based on the rating level set.”); *supra* Section V.B. Indeed, V-chips have been mandated in *all* “televisions produced for sale in the United States” since 2000. Ex. 1001, 1:19-22.

68. A POSITA would have recognized that Sullivan’s PVR implements functionality commonly performed by a V-chip. Sullivan, [0053], [0096]-[0101]. For example, 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. Sullivan, [0053], [0096]-[0101]. The V-chip was 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]. Given the V-chip’s prevalence in televisions, 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 V-chips were well known to perform the desired functionality, including extracting a program rating from the VBI and preventing access to restricted content based on its rating and the programmed acceptable rating parameters. Sullivan, [0095], [0098], [0101];

Leung, [0003], [0065], [0078], [0084].

69. A POSITA would have had a reasonable expectation of success in implementing Leung's V-chip in Sullivan's television. Sullivan discloses that the television content includes a rating in the VBI, and V-chips are designed to use the VBI to identify the rating factors for a television program. 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. 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.

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

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

71. As depicted in Figure 13 below, Sullivan discloses that if "a user requests content ... from a ratings enabled media" (e.g., "cable television services" and "video on demand") 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 the content is blocked, the user may still access it if the user is authorized to do so, for example, by entering “an access code, password or the like.” Sullivan, [0074]. “[U]nauthorized viewers, such as children, who do not possess the necessary password” cannot access the content. Sullivan, [0074].

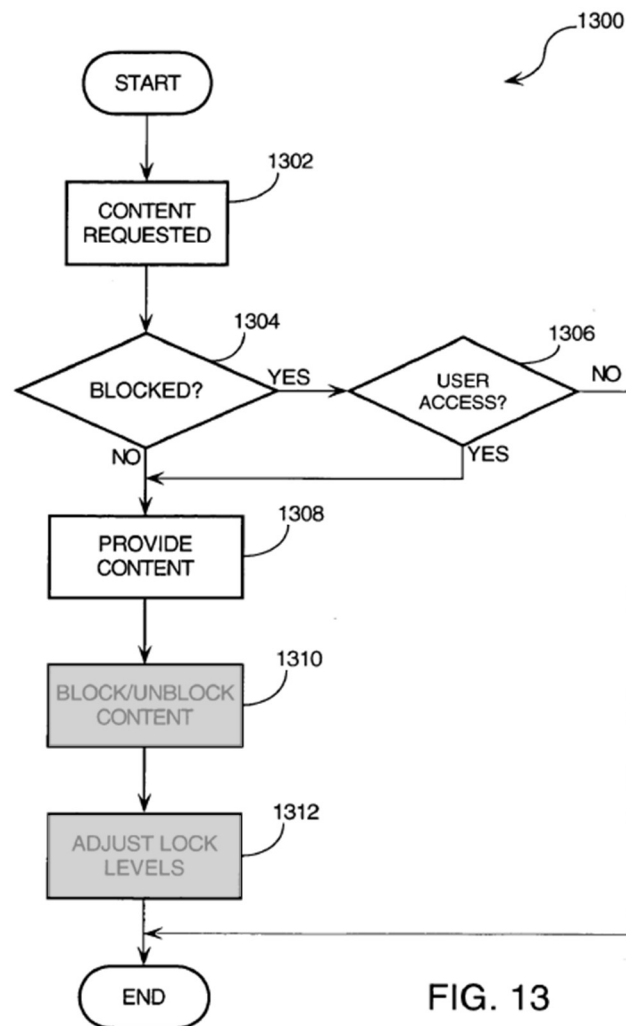


FIG. 13

Sullivan, FIG. 13 (annotated).

72. 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 then 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].

73. 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 or the like.” Sullivan, [0072]-[0074], [0077]. Because Sullivan teaches providing each PVR user a “unique password” and creating exception lists identifying users that are allowed to view content otherwise blocked based on its rating, 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 passwords

associated with the users identified on the associated exception list. Sullivan, [0099]-[0101]. A POSITA would have seen this as beneficial 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. Sullivan, [0006], [0088]-[0089], [0099]-[0101].

74. 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. For example, 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]. A POSITA would have been motivated to maintain this familiar user experience of using passwords

to override a V-chip blocking policy in Sullivan's system.

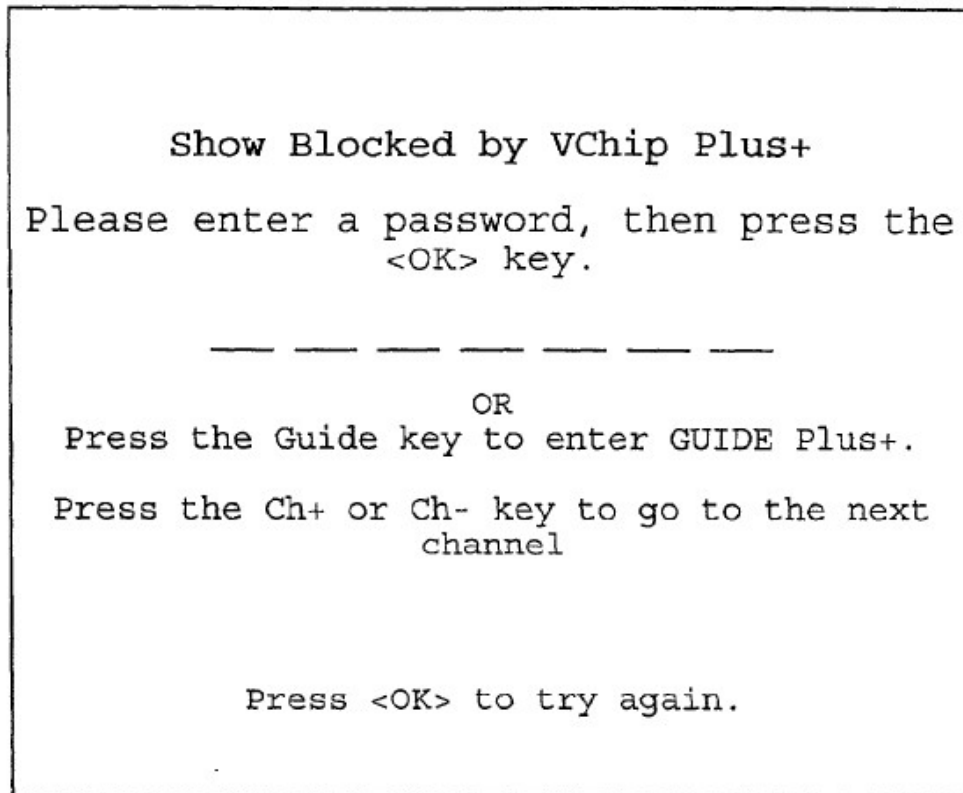


FIG. 66

Leung, FIG. 66.

75. A POSITA would have reasonably expected success in the combination because it would have required implementing only conventional techniques for determining whether an entered password matches a password associated with a user identified on the requested content's exception list and, if so, overriding a blocking signal. Indeed, Sullivan already discloses that each user "enter[s] 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 in combination with Sullivan's exception lists. Sullivan, [0089]-[0090]; Leung, [0082]-[0090]. Moreover, storing multiple unique passwords, each of which may provide access to blocked content was already well known. For example, a POSITA would have known from state-of-the-art references like Craner how to implement 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 ... or on a network location" and granting the user access to the requested content "[i]f the access code is valid." Craner, 20:24-21:20, FIG. 15.

76. If Patent Owner argues that Sullivan's exception lists are not rating based access control, a POSITA would have further found it obvious to modify Sullivan's exception lists by allowing parents to identify users *and* a rating associated with the content for each identified user. A POSITA would have been motivated to do so to improve Sullivan's content control system by allowing parents to both allow users to access content who would otherwise be blocked based on its original rating *and* to block users from accessing the same content who would otherwise be allowed to access the content based on its original rating.

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 could change 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 because it would have allowed a parent to specify a rating to apply for each “sensitive user[]” when the parent disagrees with the original rating without permanently overwriting the stored rating. Sullivan, [0006], [0099].

77. 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 disclosures of 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. 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 single list that identifies both programs to block and programs to allow, despite the V-chip setting and the program’s rating, 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. 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:”**

78. Sullivan and Leung teach “[a]n apparatus for setting rating based access controls for known digital content to be played on a video playback device having a V-chip,” as I explain below.

79. Sullivan's PVR is a video playback device because it stores "television content" and allows playback of stored content on a "content viewing device." Sullivan, [0034], [0093], [0095]-[0101]. For the reasons discussed in Section VIII.B.1.a, it would have been obvious to incorporate Leung's V-chip into Sullivan's PVR such that it has a V-chip.

80. Sullivan's PVR is one type of information appliance that includes a native parental control subsystem, also called a content control system (an apparatus). Sullivan, Abstract, [0009], [0012]. This apparatus allows setting rating based access controls for known content to be played on 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 one of the users, the apparatus allows setting an exception list for this viewed content identifying "at least one user who is 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, for the reasons discussed in Section VIII.B.1.b, it would have been obvious to modify Sullivan's exception lists to identify both a user and a rating for the associated content for each identified user. Based on the stored content's rating, the V-chip's acceptable content rating parameters, and an exception list associated with the stored content, the apparatus allows authorized users to play the requested content or prevents "unauthorized users from viewing

restricted content.” Sullivan, [0074], [0077], [0089], [0095]-[0101]; *supra* Section VIII.B.1.

81. The content stored on the PVR is “known digital content” because the PVR records the content as compressed or uncompressed data on “a hard disk drive,” which is a well-known type of digital storage medium. Sullivan, [0096]-[0100] (disclosing use of MPEG-2 compression); Walls, [0003] (disclosing that a PVR’s hard disk “digitally records live television (TV) programs” for playback); Baumgartner, [0062] (describing a “hard disk drive” as “a digital storage device”). 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 VIII.B.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”**

82. Sullivan and Leung teach [1a].

83. Sullivan teaches “a rating policy management module for selectively setting rating based access control... for digital content of a digital library.” Sullivan’s PVR is one type of “hardware system” that “is controlled by a central processing system 102,” including “a central processing unit.” Sullivan, [0012],

[0031], [0033]. This processor may execute “instructions resident in memory” that implement Sullivan’s content control system. Sullivan, [0031], [0094]. These instructions, for example, allow the addition of recorded content and an associated rating to the PVR’s hard disk drive, the creation of a profile and a “unique password” for each user or group of users of the PVR, and the creation of an exception list identifying one or more users and a content rating. Sullivan, [0046]-[0050], [0088]-[0090], [0095]-[0101]; *supra* Section VIII.B.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. This aligns with the ’879 patent’s disclosure of a rating policy management module. Ex. 1001, 7:55-58, 11:1-37. At a minimum, such a module would have been obvious, as modules were well-known ways to organize functionality for software programs.

84. Sullivan’s PVR permits control of “digital content of discloses a digital library” of digital content because the PVR includes a hard disk drive digitally storing television content for later viewing. Sullivan, [0095]-[0101]; *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].

85. Sullivan’s PVR discloses permits control of “digital content of a

digital library” because the PVR includes a hard disk drive digitally storing television content for later viewing by an authorized user. Sullivan, [0095]-[0101]; *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].

86. For the reasons discussed in Section VIII.B.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.” 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). Sullivan, [0099]-[0100]; *supra* Section VIII.B.1.b. Additionally, for the reasons discussed in Section VIII.B.1.b, it would have been obvious to modify Sullivan’s exception lists to identify both a user and a content rating associated with each identified user and to apply this content rating whenever the corresponding user attempts to access the associated content.

- 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,”**

87. Sullivan teaches [1b].

88. 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.” These instructions, for example, determine whether requested content is blocked and, if so, overrides the default V-chip policy if the user enters a password that corresponds to a user allowed to access the content based on the policy specified by the associated exception list. *Supra* Section VIII.B.1.b. This aligns with the ’879 patent’s disclosure of a rating policy enforcement module. Ex. 1001, 7:34-40. At a minimum, such a module would have been obvious, as modules are well-known ways to organize functionality for software programs.

89. 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.” 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].

90. 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 plurality of users. Sullivan, [0099]-[0100]; *supra* Section VIII.B.1.b. For example, 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 content control system may allow access” when the user enters an access code or password that authorizes access to the content, such as when the user appears on an exception list. Sullivan, [0074], [0077], [0089]-[0090], [0099]-[0100]; *supra* Section VIII.B.1.b.

- 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,”

91. Sullivan and Leung teach [1c].

92. Sullivan discloses that first and second users of the plurality of users have different media rating requirements. 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), “who may, in turn, have more restrictive acceptable content rating parameters than would an adult.” Sullivan, [0088], [0099].

93. Sullivan teaches that the first and second users have different media ratings associated with a same specific digital content. 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 exception list for this program, will be blocked access to the program based on its TV-14 rating, whereas the thirteen year old user, who has “another password” and appears on the exception list, is allowed access to the program upon entering the associated password. Sullivan, [0006], [0088]-[0089], [0099]-[0100]; *supra* Section VIII.B.1.b.

94. Moreover, for the reasons discussed in Section VIII.B.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, for example, so that a parent's decisions regarding whether to grant or deny each child access to particular content would not be impacted if the default ratings-based policy enforced by the V-chip changes. Sullivan, [0045]; *supra* Section VIII.B.1.b.

- 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,”**

95. Sullivan teaches [1d].

96. Sullivan discloses that each user or group is provided “a unique password” to access content on the PVR. Sullivan, [0099]. Sullivan discloses that “a seven year old child [(a second of the two users)] may have one password ... while a thirteen year old [(a first of the two users)] may have another password.” Sullivan, [0099]. 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 prevent them from viewing 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),”

97. Sullivan or Sullivan and Craner teach [1e].

98. As discussed for [1d], the first user’s password is a first authentication code. Sullivan, [0099]. 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. Sullivan, [0074], [0077]-[0078], claim 19.

99. If the Patent Owner argues that Sullivan does not teach a PIN, a POSITA would have found it obvious to combine Sullivan and Craner to implement Sullivan’s password/access codes for each user, including the first authentication code, as a PIN. PINs were well-known passwords/access codes used to grant access to restricted television content, as evidenced by both Leung’s and Craner’s use of a PIN to override a default rating policy. Leung, Abstract, [0181], FIG. 69; Craner, 9:3-7, 10:28-46, FIGS. 3-4. For example, Craner discloses a PIN as one type of “parental control access code” and discloses creating PINs for “users (e.g., children) of the system in order to access media and other assets.” Craner, 9:3-7, 10:28-46, 11:36-43, FIG. 5. Craner discloses that the system maintains “a list of authorized parental control access codes” and uses this list to validate the entered code. Craner, 21:8-20. A user may enter their PIN on a user interface like

the one below. Craner, 10:28-46, 11:36-43, FIG. 5.

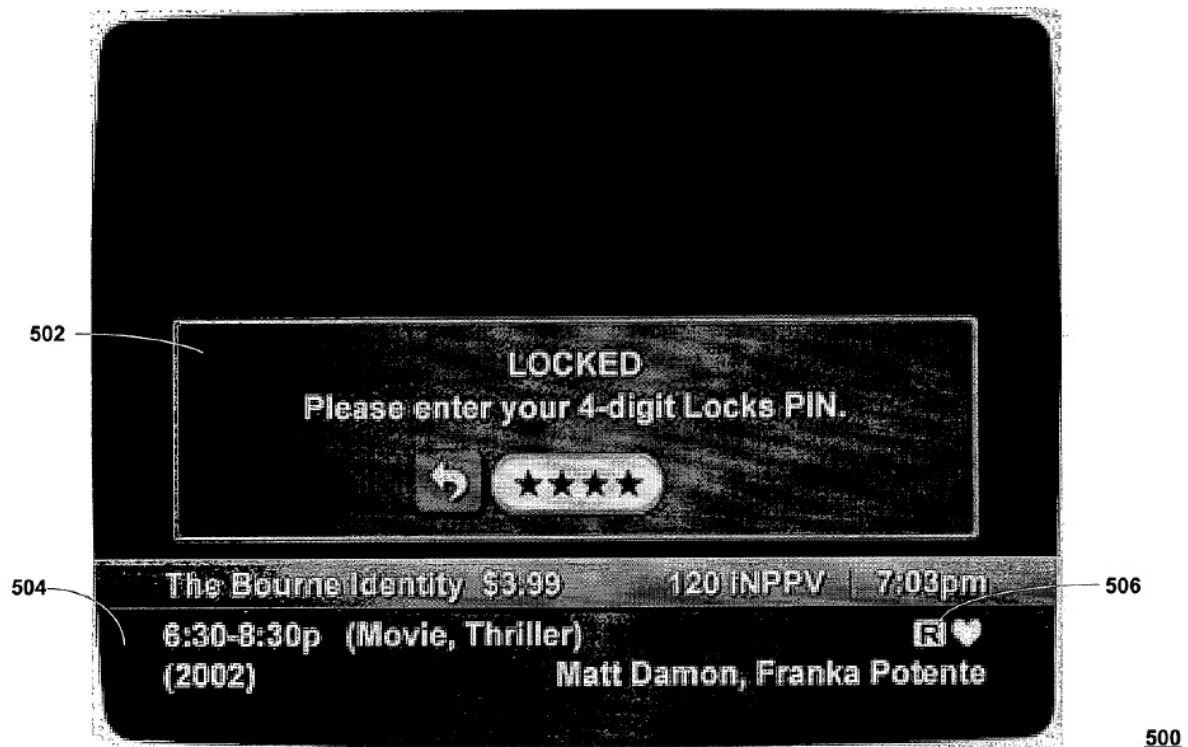


FIG. 5

Craner, FIG. 5.

100. A POSITA would have been motivated to use PINs as Sullivan's passwords/access codes to facilitate the entry of the password/access code. Sullivan discloses using a "remote control device" as an input device, and remote controls commonly included a numerical keypad and lacked letter keys. Sullivan, [0069]; Leung, [0090], FIG. 6. A POSITA would have known from contemporaneous references like Jarman that entering a PIN would be easier than entering an alphanumeric password, because the typical remote control's numerical keypad would have facilitated entering the PIN. Jarman, [0036] ("Due to the

inherent limitations of most current remote control devices, which typically only have numeric keys and are lacking in alphabet keys, the ... password may be limited to numeric characters for convenience.”). Moreover, Sullivan contemplates using the passwords/access codes for small children, who would have been more likely to remember their password if it were in the form of a PIN instead of an alphanumeric sequence. Using a PIN was a well-known “method for verifying the identity of a user.” Novack, [0007]. 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.

101. A POSITA would have had a reasonable expectation of success implementing Sullivan’s password/access code as a PIN. PINs were well-known forms of passwords/access codes commonly used in the context of parental control. Leung, [0181], FIG. 69; Craner, 9:3-17, 11:36-43, FIGS. 3-5; Jarman, [0036]. Indeed, the ’879 patent recognizes the use of “a PIN code” in prior art systems. Ex. 1001, 1:60-63, 2:44-48. Implementing Sullivan’s password/access code as a PIN would have required a POSITA to apply only conventional techniques of transmitting data entered using a remote control’s numerical keypad to the PVR for verification.

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

102. Sullivan or Sullivan and Leung teach [1f].

103. 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, [0067], [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 will only allow 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 VIII.B.1.b. 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]. 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, 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. *Supra* Section VIII.B.1.b.

- 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.”**

104. Sullivan and Leung teach [1g].

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.” Sullivan's exception lists (implemented according to Leung, *supra* Section VIII.B.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, in order 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”). 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. In order 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].

106. 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]. 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."**

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

108. Sullivan discloses that "multiple user profiles may be created and stored for individual users or groups of users." Sullivan, [0088]. Sullivan also discloses that "the exception list is stored and associated with the stored content for controlling access to the content." Sullivan, [0099]-[0100]. This stored content corresponds to the digital content of the digital library. *Supra* [1a]. 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].

109. If Patent Owner argues that Sullivan does not teach this database, 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.

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

110. Sullivan teaches the additional limitations of claim 3.

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. 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]. 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]. For example, 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].

112. 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. A POSITA would have been motivated to do so, for example, 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]. 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 in order to avoid manually entering the policies, which can be cumbersome since the policies may not all be viewable in one place on the first PVR. 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.

4. Independent Claim 4

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

113. Sullivan and Leung teach "A method in a computing system for creating specific rating policies for digital media access."

114. Sullivan discloses implementing its PVR using a "hardware system 100" (computing system) that allows an authorized user to set ratings-based parental locks, create "multiple user profiles," and create an exception list associated with each instance of content on the PVR. Sullivan, [0031]-[0033], [0039]-[0040], [0046]-[0051], [0053], [0088]-[0089], [0099]-[0100]. For the reasons discussed in Section VIII.B.1.a, it would have been obvious to implement Sullivan's ratings-based parental locks using Leung's V-chip. The exception lists, for example, are specific rating policies for access to digital media on the PVR. *Supra* [1a].

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

115. Sullivan teaches [4a].

116. 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, [0094], FIG. 1. The information appliances described in Figure 1 include “a central processing unit such as a microprocessor ... for executing programs, performing data manipulations[,] and controlling the tasks of the hardware system 100.” Sullivan, [0031], [0033]. A POSITA would have understood that Sullivan’s PVR, under the control of this hardware system having the memory and the processor, performs the functions discussed for [4b]-[4j].

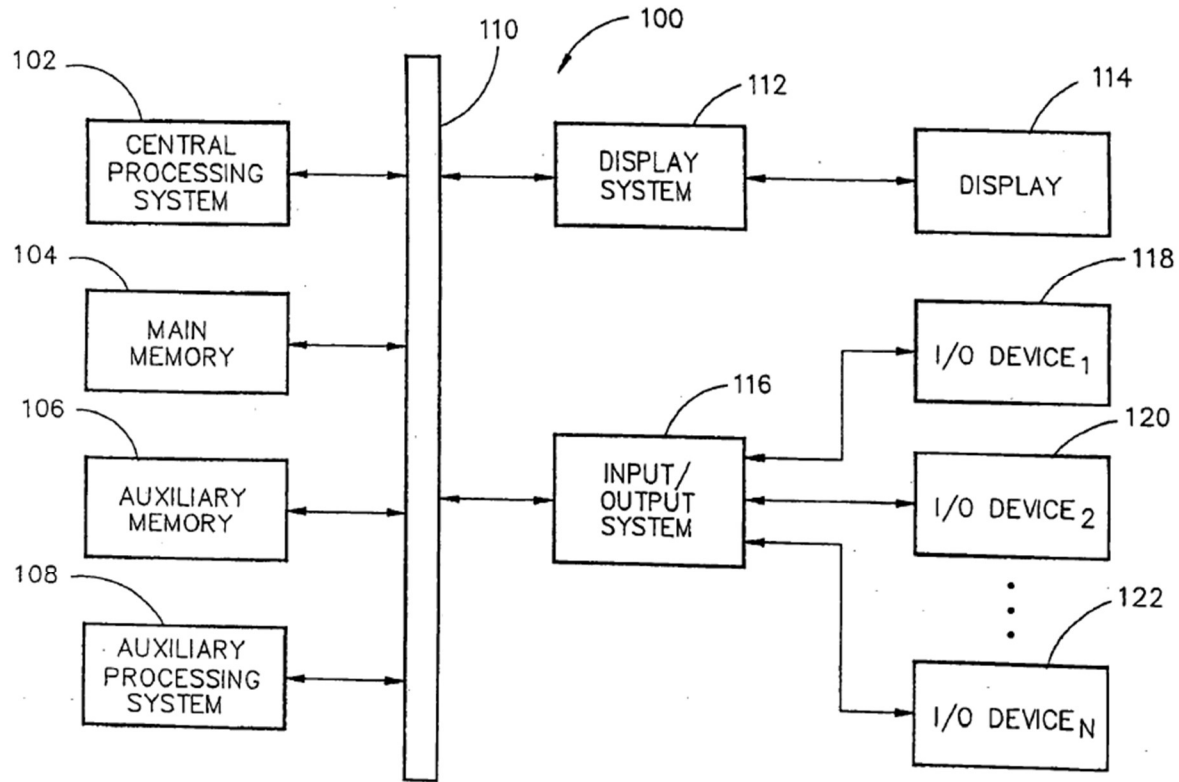


FIG. 1

Sullivan, FIG. 1.

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

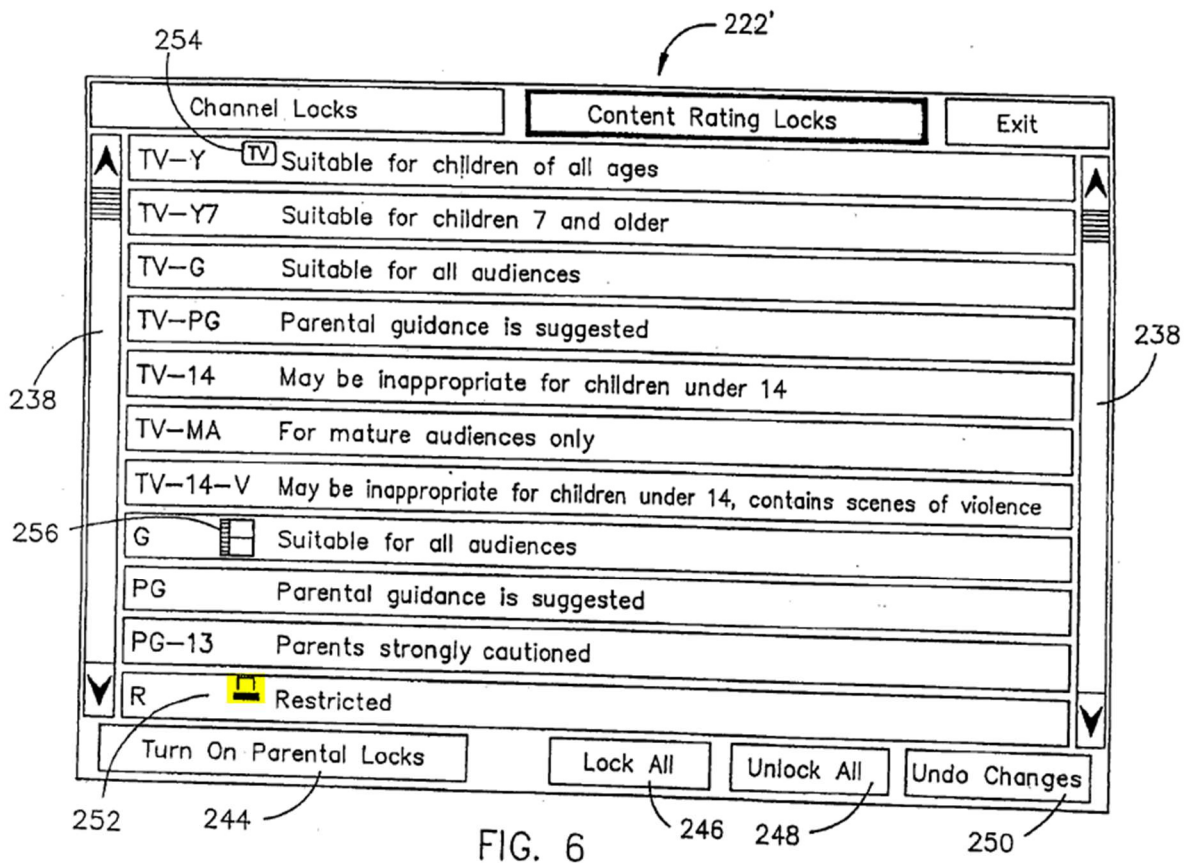
[4c]: “displaying the rating based media access policy to a user;”

117. Sullivan teaches [4b] and [4c].

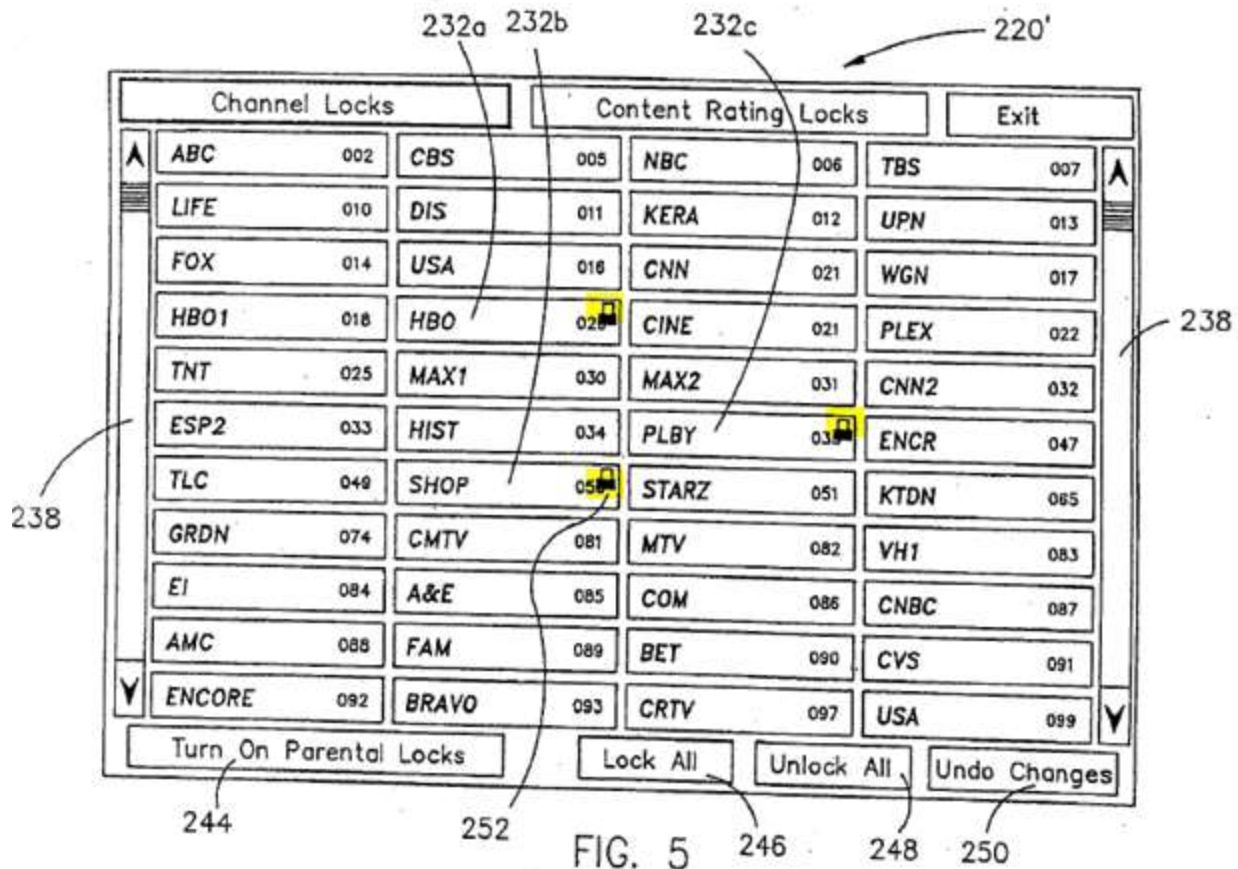
118. Sullivan discloses “retrieving media information from the memory comprising a rating based media access policy for a digital content” and “displaying the rating based media access policy to a user” because, after a user selects “the parental locks feature” to access the “parental locks interface,” 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.” Sullivan, [0046]-[0048]. “The user may also be informed of which user profile is currently selected, if any, or other status of parental locks.” Sullivan, [0048]. Sullivan uses the term “parental locks” interchangeably with “acceptable content rating parameters” and “parental lock levels.” Sullivan, [0064]. This retrieving of previously saved user settings or profiles from memory and displaying the user settings (e.g., exception lists), profiles, and parental locks information in the parental locks interface teaches retrieving media information from the memory comprising a rating based media access policy for a digital content and displaying the policy to a user. For example, Sullivan may display “a visual indication,” highlighted below, of the “ratings that have been selected to be locked,” where the visual indication indicates the rating based media access policy for a digital content because it indicates the digital content that will be allowed or blocked based on its media rating. Sullivan, [0041], [0053], [0072]-[0074], [0077], FIG. 6. As Sullivan explains: “FIGS. 5 and 6 also depict an embodiment providing a visual indication of the channels and ratings that have been selected to be locked. Channel cells 232a, 232b, and 232c, are illustrated in FIG. 5 with optional padlock icon 252 appearing therein. In FIG. 6, the R rating is shown in a similar manner as being locked. Any manner of differentiating locked channels from unlocked

channels and locked ratings from unlocked ratings may be employed, either as an alternative or in addition to a graphic or iconic indication such as padlock icon 252.” Sullivan, [0041].



Sullivan, FIG. 6 (annotated).



Sullivan, FIG. 5 (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,”

119. Sullivan and Leung teach [4d].

120. 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.” Sullivan’s television content stored in the hard disk drive of a PVR 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 an instance of 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].

121. 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.” 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]. This override list can be accessed and edited by an authorized viewer. 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].

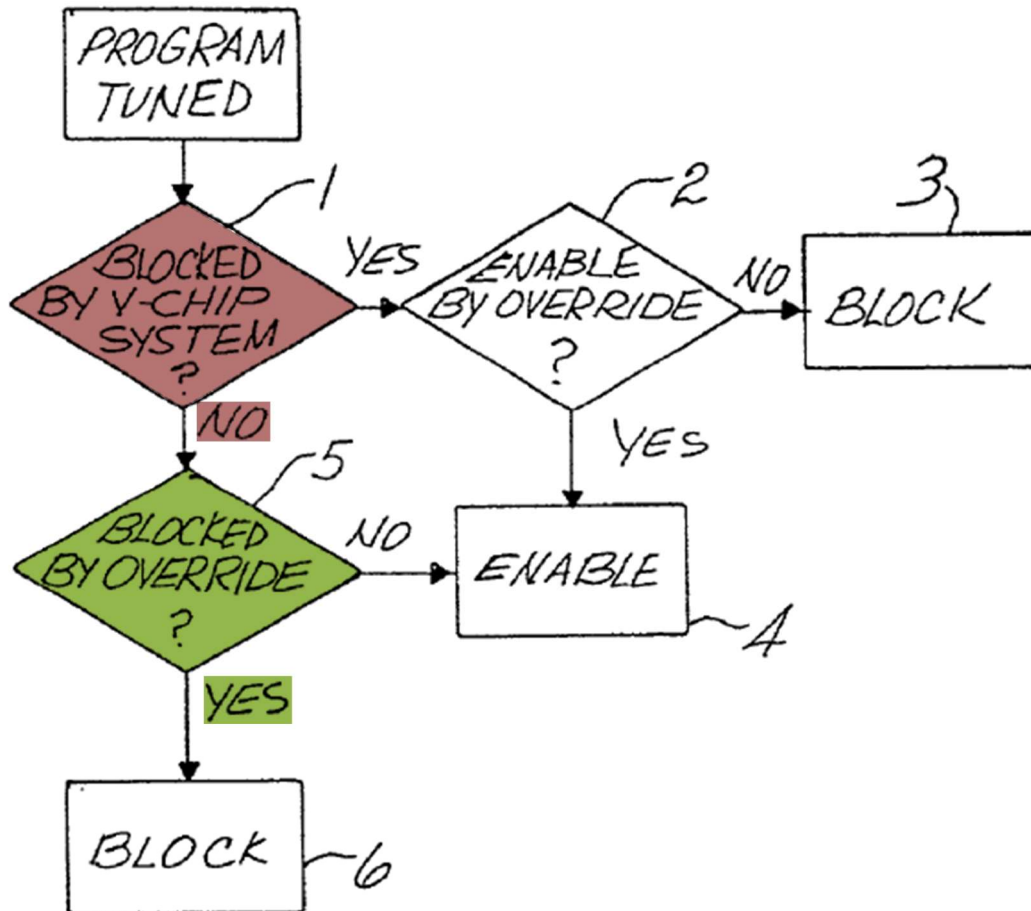


Fig. 1

Leung, FIG. 1 (annotated).

122. 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]. As Sullivan recognizes, “a user such as a parent or the like 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]. Accordingly, 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.

123. A POSITA would have been motivated to provide a parent, upon viewing such content, the ability to either allow *or* block a particular child’s access to that content without changing that user’s acceptable content rating parameters. 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 “by comparing the rating of the television program with the existing parental lock levels for that user ... and adjusting the parental lock levels accordingly.” Sullivan, [0090]-[0092].

124. 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. 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.

125. 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, a POSITA would have viewed combining Sullivan and Leung as requiring only conventional programming techniques to modify Sullivan's existing exception list disclosure for the purpose of blocking access to users that would otherwise be allowed access in a similar way to Leung's blocking override list.

126. Additionally, for the reasons discussed in Section VIII.B.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]. Each different media rating in the exception list constitutes a different rating based access control policy override action for the corresponding user. This would have been beneficial, for example, so that a parent's decisions regarding whether to grant or deny each child access to particular content would not be impacted if the default ratings-based policy enforced by the V-chip changes. Sullivan, [0045]; *supra* Section VIII.B.1.b.

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

127. Sullivan teaches [4e].

128. Sullivan's PVR receives the override actions from “[a]n authorized user (e.g. a parent or guardian),” who is different 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. Only the “authorized user” (an administrator, *supra* [1b]), upon entering their password, can “adjust the parental lock levels of the parental control system for each user or group of users” and generate exception lists. Sullivan, [0090], [0099]-[0100].

- 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;”**

129. Sullivan teaches [4f].

130. Sullivan discloses that each of the users has a “unique password”

(authentication code) associated with their profile. Sullivan, [0074], [0077], [0089]-[0090], [0099]; *supra* [1d].

- 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”**

131. Sullivan and Leung teach [4g].

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. 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].

133. 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]. Future playback of the digital content stored on the PVR and associated with each exception list is allowed or blocked consistent with the stored policy override action. Sullivan, [0099]-[0100]. 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].

- 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,”**

134. Sullivan and Leung teach [4h].

135. Sullivan discloses that the first viewer is allowed to access the specific digital content based upon the first authentication code for the reasons discussed for [1d].

136. 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. 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]. A POSITA would have been motivated to implement this functionality to block the second viewer’s access

to content whose rating the parent has deemed not “stringent enough” for that user. Sullivan, [0006]. A POSITA would have had a reasonable expectation of success for the reasons 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.

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

137. Sullivan and Craner teach [4i] for the reasons discussed for [1e].

- j. **[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.”**

138. Sullivan and Leung teach [4j] for the reasons discussed for [1g].

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.”**

139. Sullivan teaches “validating the authentication codes of the first viewer and the second viewer.”

140. Sullivan teaches that, if a user selects content that is blocked “because its content rating exceeds the rating threshold delineated by previously set acceptable content rating parameters of the content control system,” the user must “enter an access code, password[,] or the like 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]. Sullivan also discloses that, “if incorrect passwords are entered a predetermined number of times, the system may be instructed to disable access to the media.” Sullivan, [0075]. Accordingly, a POSITA would have understood that Sullivan validates the authentication codes of the first and second viewers to determine whether to allow or block access to the requested content. If Patent Owner argues it is not disclosed, it at least would have been obvious to ensure that the system applies the correct parental locks associated with each user’s authentication code.

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

141. As discussed for [1e], it would have been obvious to implement a user’s unique password as a PIN. For the same reasons discussed for [1e], it would have been obvious to make each user’s password, including the first and second authentication codes, a PIN.

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

142. Sullivan and Craner teach that “the authentication codes comprise biometric information.”

143. Similar to Sullivan, Craner discloses that “users may be authenticated ... using a standard username and password combination.” Craner, 11:48-58; Sullivan, [0089]-[0090]. Craner also discloses that, alternatively, users may be authenticated 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.

144. A POSITA would have found it obvious to combine Sullivan and Craner such that the authentication codes for the first and second users comprise biometric information. A POSITA would have been motivated to do so because Craner discloses that using biometric information in combination with the verification module beneficially allows access to be granted “without the use of a manual parental control access code entry.” Craner, 9:17-30. Given that Sullivan’s authentication codes are frequently used by children who may be more likely to forget their password/access code, a POSITA would have seen biometric information (e.g., fingerprint) as beneficial so that the users could be verified even if they forgot their password. Moreover, a POSITA would have recognized that

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].

145. A POSITA would have had a reasonable expectation of success in combining Sullivan and Craner to implement authentication codes comprising biometric information. Using biometric information, such as via “a fingerprint reader for obtaining the fingerprint of the user” in the remote control, was a well-known technique for applying user-based parental access controls. Novack, [0013]-[0014], [0030]-[0031]. Implementing Sullivan’s authentication codes using biometric information would have required a POSITA to apply only conventional techniques (a biometric reader) to validate the user.

d. Claim 8: “The method of claim 4, further comprising displaying the media information, wherein the media information comprises a media rating.”

146. Sullivan teaches “displaying the media information, wherein the media information comprises a media rating.”

147. 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 content recorder (e.g., PVR) displays the “parental locks interface” including the “user profiles.” As Sullivan explains, “[i]f the user wishes

to open a preexisting user profile ..., the selected profile is opened.” Sullivan, [0048]. Sullivan teaches that, through the parental locks interface, “[t]he computer may textually or graphically display the level of parental locking,” which includes “the material and/or channels to be locked.” Sullivan, [0045]. Sullivan’s parental locks interface is illustrated in, for example, Figure 4. As shown, Sullivan’s interface includes a number of “TV or movie rating[s] and a brief description of the rating[s].” Sullivan, [0039]. Through this interface, “a user may select particular ratings to lock and unlock.” *Id.* In this manner, Sullivan’s interface displays media information that “comprises a media rating.”

148. If Patent Owner argues Sullivan does not teach “displaying ... a media rating,” a POSITA would have been motivated and found it obvious to include a media rating in Sullivan’s parental locks interface based on Leung. Leung describes a “parental control user interface” that, like Sullivan’s parental locks interface, allows a parent to “override” an existing rating “for individually selected television programs.” Leung, Abstract, [0076]-[0077].

149. Leung’s parental control 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].

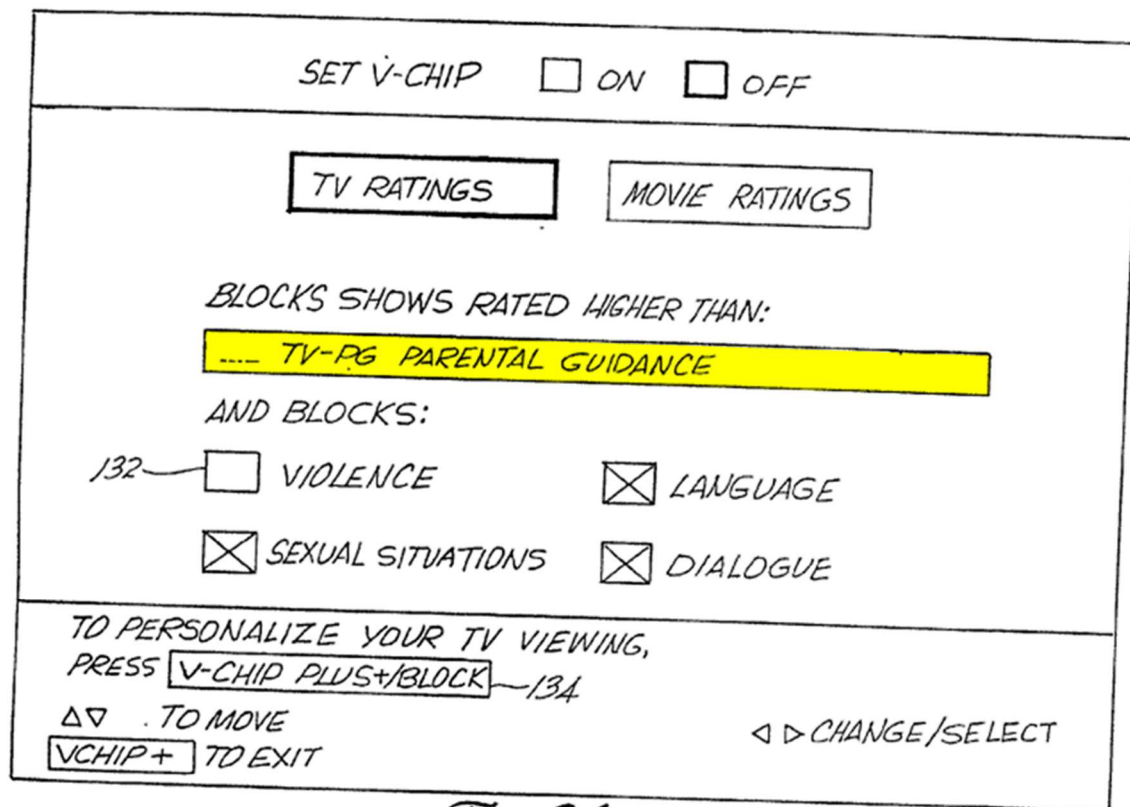


Fig. 24

Leung, FIG. 24 (annotated).

150. Leung also describes the “GUIDE mode” for its parental control interface, illustrated in Figure 51 below. Leung, [0049], [0152], [0174]. As shown, the interface lists content, including media ratings for each content. From this interface, “[i]ndividual shows or entire channels may be blocked,” and “blocked shows or channels are in dark gray.” Leung, [0174].



FIG. 51

Leung, FIG. 51.

151. From Leung, a POSITA would have been motivated and found it obvious to implement Sullivan's parental locks interface to include a media rating for each content. A POSITA would have found it obvious 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. 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]. A POSITA would have had a reasonable expectation of 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].

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

152. Sullivan or Sullivan and Leung teach the additional limitations of claim 9.

153. 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 content recorder displays the “parental locks interface” including the “user profiles.” Through Sullivan’s parental locks interface, “a user may select particular ratings to lock and unlock.” Sullivan, [0039], [0045].

Additionally, Sullivan also discloses that a user may set 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]. One channel lock overlay

is depicted in Figure 3, below. 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].

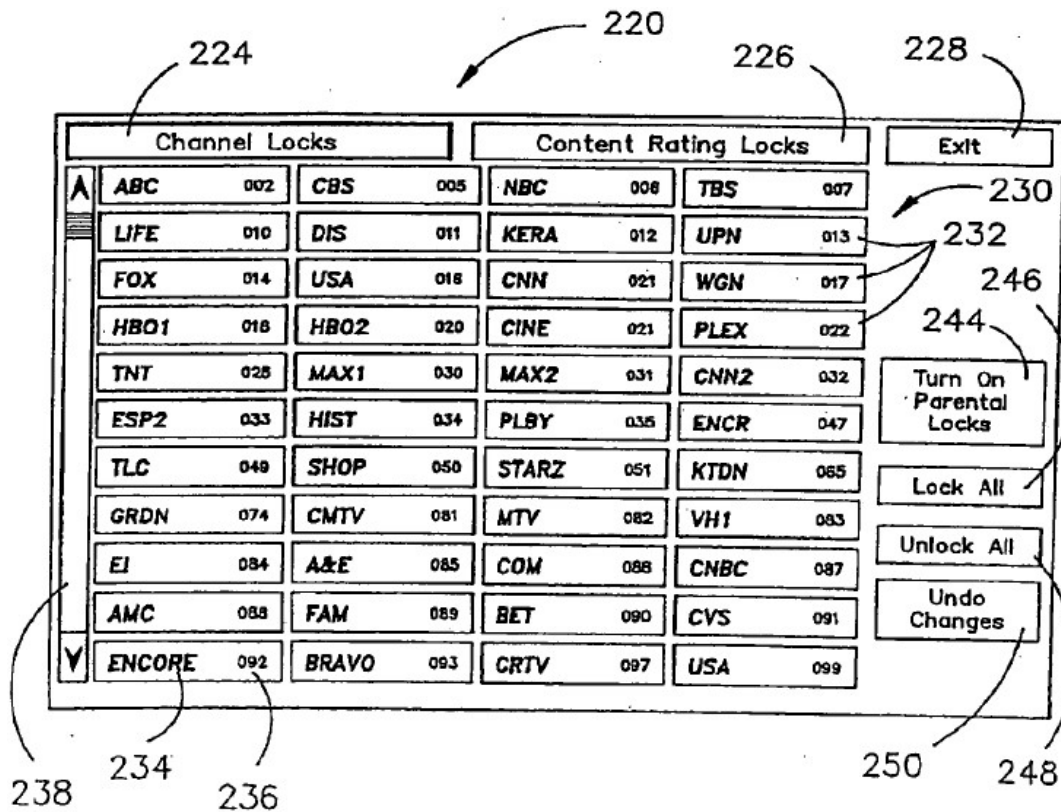


FIG. 3

Sullivan, FIG. 3.

154. Additionally, a POSITA would have been motivated and found it obvious to include “a media owner” in Sullivan’s parental locks interface based on Leung. As explained for claim 8, Leung describes a “parental control user

interface” that, like Sullivan’s parental locks interface, 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, [0049], [0152], [0174], FIG. 51).

155. As shown in Figure 51 below, 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. A POSITA would have recognized that, in many instances, a channel on which content is displayed is also “a media owner” of the content. From this interface, Leung explains, “[i]ndividual shows or entire channels may be blocked,” and “blocked shows or channels are in dark gray.” Leung, [0174].



FIG. 51

Leung, FIG. 51.

156. From Leung, a POSITA would have been motivated and found it obvious to implement Sullivan's parental locks interface to include a media owner for each content. A POSITA would have found it obvious 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. 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]. A POSITA would have had a reasonable expectation of 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.

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.”

157. 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]. 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].

158. And, as explained for [4d], Sullivan and Leung teach the “second, different, ... policy override action” because a POSITA would have found it

obvious to combine Sullivan and Leung to add the second viewer to an “exception list” associated with the same specific digital content that blocks the second viewer from viewing otherwise allowable content. *Supra* [4d]. 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.”

159. 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 also 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). To this end, Sullivan envisions “profiles” that are created “for individual users or *groups of users*,” and that “acceptable content rating parameters” are “set specifically for that user or *group of users*.” Sullivan, [0088] (emphases added). For example, parameters may be set “for different children (or age groups).” Sullivan, [0047]. Accordingly, while Sullivan provides “a thirteen year old” being added to an exception list as an example, a POSITA would have understood that Sullivan’s

teaching of an exception list likewise allows parents to add one of the groups previously discussed that includes this thirteen-year-old (e.g., “Children”).

Sullivan, [0090], [0099]-[0100], FIG. 15.

6. Independent Claim 12

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

160. Sullivan teaches [12pre] for the reasons discussed for claim 1.

Sullivan’s PVR, for example, is a computing system that implements a method for enforcing rating based media access policies set 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:”**

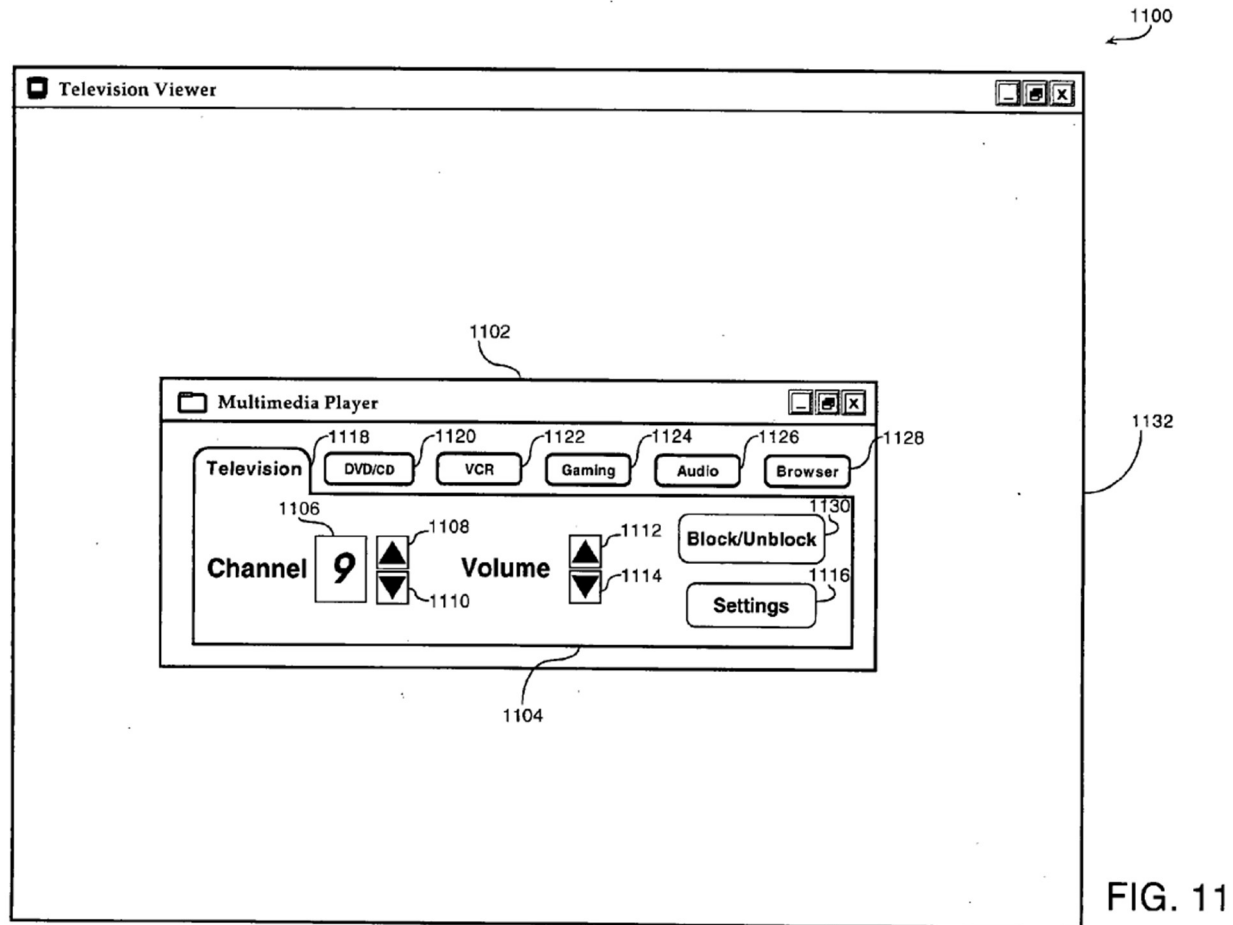
161. Sullivan and Leung teach [12a] for the reasons discussed in Section VIII.B.1.a and for [1pre]-[1a]. Sullivan’s PVR, implemented with Leung’s V-Chip, is a “video playback device having a V-Chip that specifies [a] default rating based access policy.” *Supra* Section VIII.B.1.a, [1pre]-[1a].

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

162. Sullivan or Sullivan and Leung teach [12b].

163. Sullivan discloses a user interface “displayed to the user” that “include[s] an on-screen control panel 1102 for controlling access to media by the

information appliance” and includes “display fields” (e.g., “Channel”) and control buttons, “which function as on-screen visual representations of controls of the information appliance or, alternately, peripheral devices attached thereto that provide access to one or more media.” Sullivan, [0066]. The user interface provides buttons that, “when selected, 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 in the example depicted below, which shows a television viewing application, Sullivan’s control panel displays the selected channel number. Sullivan, [0072], FIG. 11. While only the “Television” tab of the display is illustrated, Sullivan also envisions tabs for a “DVD/CD,” “VCR,” “Gaming,” Audio,” and “Browser,” which a POSITA would have recognized would likewise display appropriate controls. Sullivan, FIG. 11.

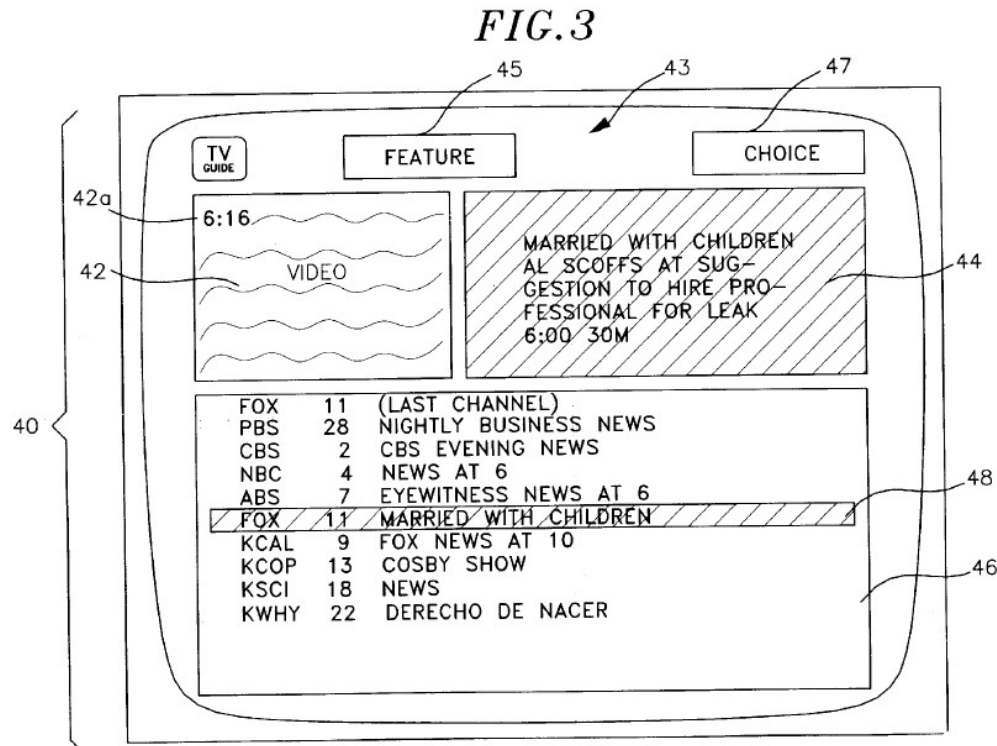


Sullivan, FIG. 11.

164. A POSITA would have understood that, when using a PVR implementing the content control system, a user interface would include a button that, when selected, displays the PVR viewing application through which a user could select “to view a specific instance of audio/visual content.” Sullivan, [0095]-[0101]. Moreover, a POSITA would have understood that the PVR viewing application would include selectable metadata corresponding to recorded television programs stored at the PVR, to aid a user in selecting content. 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, [0034], FIG. 20a.

165. If Patent Owner argues Sullivan does not disclose this, Sullivan and Leung would have rendered obvious a user interface displaying metadata corresponding to the recorded television programs at the PVR, where a user could select the metadata “to view a specific instance of audio/visual content.” For example, 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”), 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 (disclosing a user interface depicting metadata for television programs that can be selected by the user). For example, Figure 3, below, includes a display of 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 and “highlight one of the program listings displayed.” Yuen, 5:62-63, 6:18-29. “When the viewer finds a program that the viewer wishes to watch,” the viewer presses a button on the remote control to display that program. Yuen, 2:35-42, 7:34-40, 11:23-25.



Yuen, FIG. 3.

166. A POSITA would have been motivated to incorporate a display of metadata, similar to Leung's, where the user interface lists the titles of available television programs stored on the PVR and other relevant program metadata to facilitate user selection of the desired program for playback through selection of the listed program metadata. Such a display of metadata for available programs was well known at the time and would have been a beneficial and familiar user interface for users to easily navigate through the available content and control selection of the desired content on the PVR. Barton, [0093]-[0094], [0098], FIGS. 8-10 (disclosing the display of titles corresponding to programs on a DVR for selection and playback); Baumgartner, [0034], FIG. 20a. 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 to view.

167. A POSITA would have had a reasonable expectation of success in displaying metadata for selection because Sullivan already discloses displaying channels to select in the context of a television application, and the PVR includes a hard disk drive for storing television content "from a television receiver." Sullivan, [0096]-[0100]. Given the prevalence of similar user interfaces, incorporating the display of metadata into Sullivan's user interface for the PVR controls 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.

- 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:"**

168. Sullivan and Leung teach [12c] and subelements [12d]-[12g], addressed in the subsequent sections.

169. For the reasons 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 a specific instance of audio/visual content.” Sullivan, [0095]-[0101]; *supra* [12b].

170. Sullivan and Leung teach determining that rating based access control configured to override the V-chip default rating based access policy is enabled. As discussed for [12a], it would have been obvious to incorporate Leung’s V-chip to implement Sullivan’s specified default rating based policy. Sullivan teaches that this specified default rating based access policy applies when enabled by the “Turn On Parental Locks” button but is overridden for particular 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].

171. 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]. 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.

172. Sullivan and Leung teach subelements [12d]-[12g] “responsive to” the above determinations.

e. [12d]: “reading media information”

173. Sullivan teaches [12d] because, “upon receiving the user request” to view television content, Sullivan’s system determines if the selected 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, [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 VIII.B.1.a.

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”

174. Sullivan and Leung teach [12e] for the reasons discussed in Section VIII.B.1.b. For example, Sullivan discloses that the exception lists are stored on the PVR’s memory and associated with the content. Sullivan, [0099]-[0100]. A POSITA would have recognized that, to determine whether a user appears on the exception list, Sullivan’s PVR would read 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.” Sullivan, [0073]-[0074], [0099]-[0100]. If the content control system determines that the content is blocked by default, the content control system would read 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]. Conversely, if the system determines that content is allowed by default, the modified content control system would read 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].

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

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

175. Sullivan teaches [12f] and [12g]. 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 “unique password” (or “an access code, password[,] or the like”) associated with the user. Sullivan, [0074], [0089]-[0090], [0099]-[0100]. Sullivan teaches “validating an authentication code” and “beginning playback of the media” because, as Sullivan explains, “the user accesses the example

content ... by entering an access code or password,” and “the content control system allows the information appliance to provide the example content to the user.” Sullivan, [0077], FIG. 13.

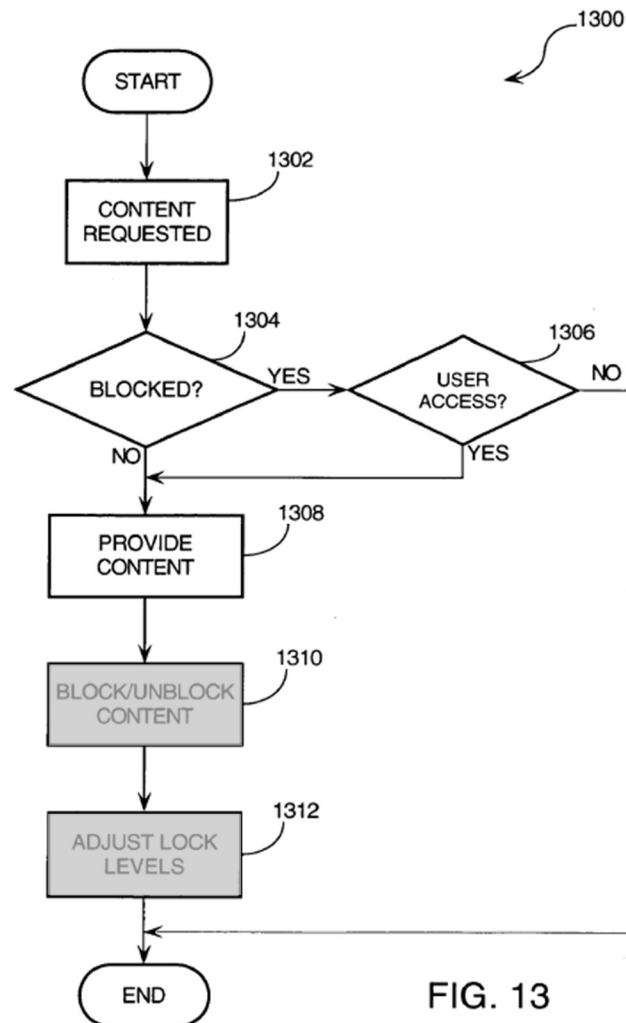


FIG. 13

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”

176. Sullivan teaches [12h].

177. Sullivan discloses that the PVR “may include a unique password for a user or a group of users,” where “a seven year old child may have one password” and “a thirteen year old may have another password.” 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” stored on the PVR. 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], as the thirteen-year-old child, and enters their own password, Sullivan’s content control system will prevent playback of the program 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].

- 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,”**

178. Sullivan teaches [12i].

179. Sullivan discloses that only “an authorized user,” upon entering their password, is allowed “to adjust the parental lock levels of the parental control

system for each user or group of users.” Sullivan, [0090]. The parental lock levels are intended “to prevent access of persons, and in particular children to inappropriate content.” Sullivan, [0064]. Accordingly, a POSITA would have understood that Sullivan’s first and second users (e.g., the thirteen- and seven-year-olds, respectively) are not administrators because their passwords do not authorize them to adjust the parental lock levels.

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

180. Sullivan and Craner teach [12j] for the reasons discussed for [1e].

- k. **[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.”**

181. Sullivan and Leung teach [12k] for the reasons discussed for [1g].

7. Dependent Claims

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

182. Sullivan and Craner teach the additional limitations of claim 13.

183. For the same reasons discussed for [1e], it would have been obvious to make each user’s password/access code (the authentication codes) a PIN.

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

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

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

185. Sullivan teaches the additional limitations of claim 15.

186. As discussed for [12e], Sullivan’s exception list is “a default rating based access policy action associated with the selected media content.” This default policy associated with the requested content is 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].

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

187. Sullivan teaches the additional limitation of claim 16.

188. As discussed for [12d], Sullivan discloses reading media information comprising the content rating of the selected media to determine whether the selected content is blocked. Sullivan, [0073]-[0074], [0099]-[0100]; *supra* [12d].

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

189. Sullivan and Leung teach the additional limitations of claim 17.

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

191. 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, for example, “to block all Horror Movies.” Leung, [0175], FIG. 54.

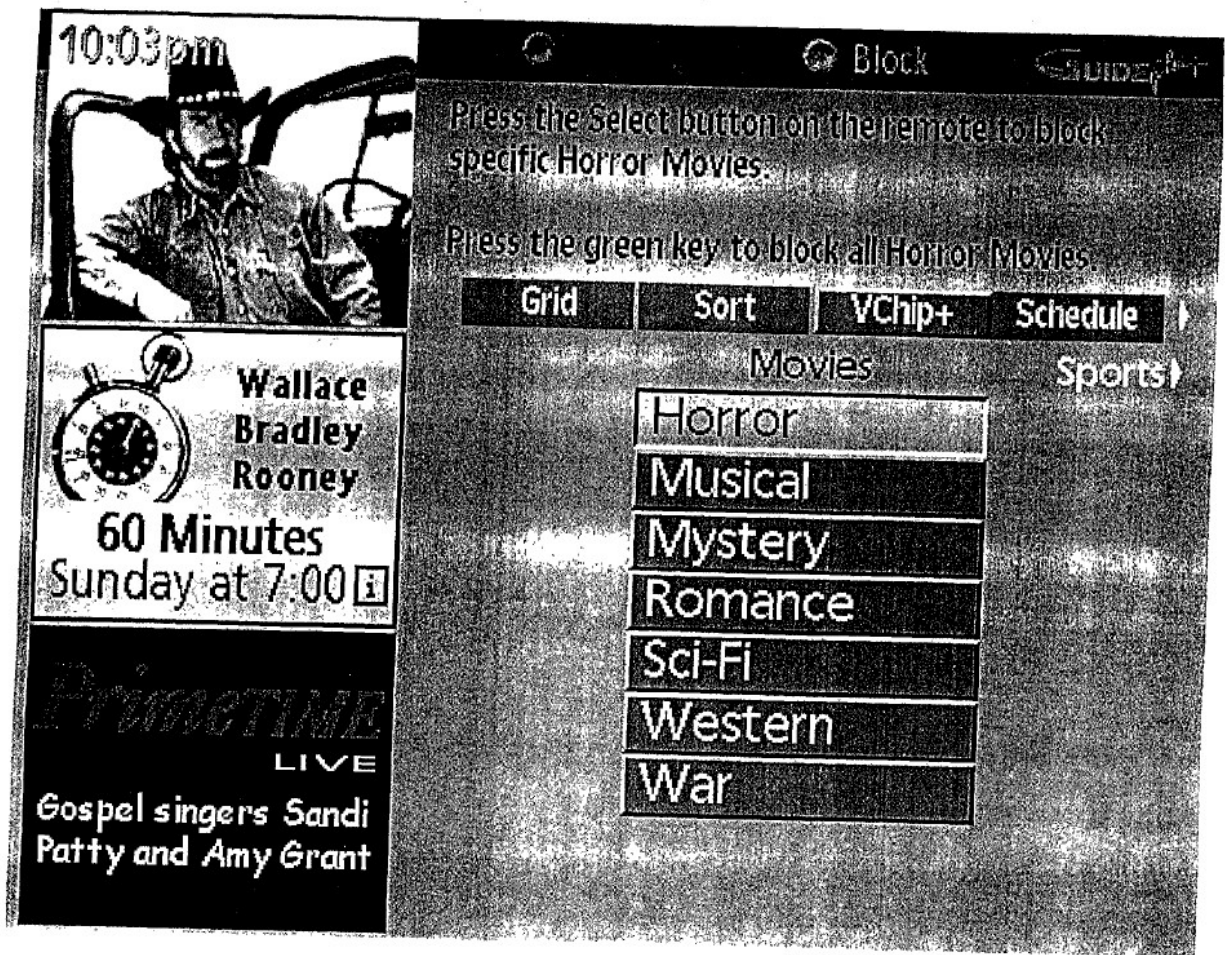


FIG 54

Leung, FIG. 54.

192. A POSITA would have been motivated to implement Leung’s genre-

based locks in Sullivan's PVR to increase the amount of control that a parent has over the content that their children watch. Doing so would have been beneficial so that, regardless of the content's rating, the parent could block its children from watching a certain genre of content (e.g., horror). Sullivan already discloses allowing a user to sort displayed content based on "category, e.g. Movies, Sports or Children's programs," and 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." Sullivan, [0082], [0091]-[0092], FIG. 15. Such genre-based control was well known. Given Sullivan's disclosure of implementing blocks based on themes, combining Sullivan and Leung to implement blocks based on genres would have been a combination of familiar elements according to known methods to predictably yield a desirable increase in flexibility and granularity in access controls. 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].

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

193. 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.” 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]. A POSITA would have been motivated and would have found it obvious to do so because Sullivan’s “channel lock overlay” allows a user to block certain channels by name (e.g., media owner), and 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]. 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].

- 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.”**

194. Sullivan and Craner render obvious the additional limitations of claim 19.

195. As discussed for [1g], Sullivan discloses authenticating a user’s authentication code. 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. 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. 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.

196. A POSITA would have been motivated and found it obvious to implement Craner’s ability to retain the most recent user’s authentication code and apply that user’s individual acceptable content rating parameters when that user accesses additional content to avoid requiring the user to input their password each

time they access content blocked for another user. 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, the user would only have to enter their password once and be able to access all the content that complies with their user profile.

197. A POSITA would have had a reasonable expectation of success. Given the similarity between Sullivan and Craner, a POSITA would have reasonably expected features from one system to work for the other. Moreover, retaining a user’s authentication code for a session would have required only conventional techniques of saving data in memory and accessing that data to confirm the access controls that apply to the current session.

IX. Conclusion

198. This declaration and my opinions herein are made to the best of my knowledge and understanding, and based on the material available to me, at the time of signing this declaration. I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 or Title 18 of the United States Code.

Date: November 21, 2024

Henry H. Houh.

Henry Houh