

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JACS Solutions, Inc.,
Petitioner

v.

Global Tel*Link Corporation,
Patent Owner.

IPR2024-00484
U.S. Patent No. 9,030,292

**DECLARATION OF RUSSELL J. NICHOLS IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW
UNDER 37 C.F.R. § 42.101**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. TECHNICAL BACKGROUND OF RUSS NICHOLS.....	3
III. THE '292 PATENT	6
IV. THE '292 PATENT PROSECUTION HISTORY	9
V. THE PRIORITY DATE OF THE '292 PATENT AND THE STATE- OF-THE-ART AT THAT TIME.....	17
VI. THE LEVEL OF ORDINARY SKILL IN THE ART FOR THE '292 PATENT	20
VII. CLAIM INTERPRETATION	25
A. The Principles of Patent Claim Interpretation (Also Known as Claim Construction)	25
B. Interpreting Certain Claim Limitations from the '292 Patent.....	26
1. Secure Facility.....	26
2. Kiosk	26
3. Biometric Verification	27
VIII. THE PRIOR ART.....	27
A. Hogg	27
B. Anderson	29
C. Shapiro.....	32
D. Rudolf.....	34
E. Swink.....	36
F. Cree.....	37

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

G.	Swanson.....	38
IX.	THE PRINCIPLES AND LAW OF PATENT INVALIDITY	39
X.	COMPARING THE '292 PATENT CLAIMS WITH THE PRIOR ART	42
A.	“A system for providing services to a secure facility, the system comprising:” (Claim 1, preamble); “A system for providing services to a secure facility, the system comprising:” (Claim 24, preamble).....	42
B.	“a kiosk located at a secure facility, the kiosk comprising a processor, display, speaker, microphone, and a camera; and” (Claim 1.a); “A kiosk for providing facility services in a secure manner, comprising: a computer processor; a memory connected to the processor via a bus; a camera connected to the bus for inputting video communications; a microphone connected to the bus for inputting audio communications; a speaker connected to the bus; a touchscreen display connected to the bus; and a network interface connected to the bus for communicating with a server via a network connection,” (Claim 15P; Claim 15.a-g); “a method for monitoring use of an interactive kiosk during a video transmission, comprising:” (Claim 22, preamble); “a plurality of kiosks located at a secure facility, each kiosk comprising a processor, display, speaker, and microphone; and” (Claim 24.a).....	44
C.	“a server that communicates with the kiosk via a network connection, the server comprising a server processor, a network interface unit, and a computer memory;” (Claim 1.b); “a server that communicates with the kiosks and a device of an outside party via one or more network connections, the server comprising a server processor, a network interface unit, and a computer memory” (Claim 24.b); and every other claim element calling out a server.	55
D.	“the kiosk being configured to receive communications from the camera and microphone and transmit audio and video of the communications to the server via the network connection” (Claim 1.c); “wherein the kiosk ... records audio and video	

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

- communications and transmits the audio and video communications to the server” (Claim 15.h); “using a camera of the kiosk to capture video of a user of the kiosk during use of the kiosk; transmitting the video to a server;” (Claim 22.a-b).....66
- E. “wherein the server records the audio and video and transmits the audio and video to a destination;” (Claim 1.d) 71
- F. “wherein the kiosk is configured to authenticate the identity of a user of the kiosk by verifying log in information entered by the user and also performing a biometric verification;” (Claim 1.e); “wherein the kiosk authenticates a user by receiving personal log in information and comparing the received personal log in information against a known personal log in information associated with the user, verifies the user's identity using a biometric verification,” (Claim 15.h).....74
- G. “wherein, after the user identity has been authenticated by the kiosk and during the transmission of the video, the server is configured to periodically extract a frame of the video and perform a check to determine if a face is present in the frame,” (Claim 1.f); “wherein, after the user has been authenticated and during a transmission of a video, the video being transmitted from the kiosk to the calling party, the server is configured to periodically extract a frame of the video; and perform a check to determine if a face is present in the frame,” (Claim 24.f); “wherein, after the user has been authenticated and during the transmission of the video, the kiosk is configured to periodically extract a frame of the video and perform a check to determine if a face is present in the frame,” (Claim 15.i); “periodically extracting, at the server, a frame of the video; performing a check after the user identity has been authenticated by the kiosk and during the transmission of the video, at the server, to determine if a face is present during the frame;” (Claim 22. d-e) 77
- H. “and the server is further configured to blur the video being transmitted to the destination when the check determines that the face is not present in the frame; and” (Claim 1.f); “and the kiosk is further configured to blur video being transmitted to a destination when the check determines that the face is not present

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

	in the frame” (Claim 15.i); “blurring the video transmission, at the server, to a destination if the check determines that the face is not present in the frame.” (Claim 22.f); “and the server is further configured to blur the video being transmitted to the calling party when the check determines that the face is not present in the frame.” (Claim 24.f)	82
I.	“wherein the destination is a device communicating with the server, and the server is configured to authenticate a user of the device.” (Claim 1.g)	87
J.	“a second kiosk located in a visitation area of the secure facility; and a local server located at the secure facility; the kiosk being configured to transmit the audio and video to the local server when the communications are intended for the second kiosk located in the visitation area; and wherein the local server is configured to record the audio and video and transmit the audio and video to the second kiosk located in the visitation area” (Claim 2).....	89
K.	“wherein the server is configured to periodically extract a frame of the video and authenticate a face in the frame against a stored identification image of the user.” (Claim 3).....	97
L.	“wherein during a singular communications session, the kiosk is configured to periodically record a frame of video and transmit the frame to the server, and wherein the server processor authenticates a face in the frame against a stored identification image of the user.” (Claim 4)	98
M.	“wherein the kiosk is configured to accept messages input by the user after the user has logged on and transmit the messages to the server, and the server is configured to provide a third party access to the messages.” (Claim 5).....	100
N.	“wherein the kiosk is configured to provide the user with at least two of: access to audio, video, and text of educational material stored on the server and/or the kiosk, access to audio, video, and text of religious material stored on the server and/or the kiosk, and the ability to order items from a list of commissary items.” (Claim 7); “wherein the kiosk provides the user with at least one	

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

- of: access to audio, video, and text of educational material; access to audio, video, and text of religious material; the ability to order items from a list of commissary items; the ability to reserve times for using the kiosk; and the ability to send text messages to third parties” (Claim 16) 102
- O. “wherein the log in information is a personal identification number” (Claim 9); “wherein the personal log in information is a personal identification number” (Claim 17).....106
- P. “wherein the biometric verification comprises a facial authentication via the camera” (Claim 10); “wherein the biometric verification comprises a facial authentication of an image captured by the camera” (Claim 18).....107
- Q. “wherein the biometric verification comprises a voice authentication via the microphone” (Claim 11); “wherein the biometric verification comprises a voice authentication of an audible phrase recorded using the microphone.” (Claim 19).....107
- R. “wherein the server is configured to detect the presence of a second face in the video frame and, while the presence of the second face is detected, the kiosk is configured to blur the video” (Claim 12); “detecting the presence of a second face in the video frame and, while the presence of the second face is detected, blurring the video transmission, at the server, to the destination” (Claim 23); “wherein the server is configured to detect the presence of a second face in the video frame and, while the presence of the second face is detected, the server is configured to blur the video being transmitted to the calling party” (Claim 28); “wherein the kiosk is configured to detect the presence of a second face in the video frame and, while the presence of the second face is detected, the kiosk is configured to blur the video” (Claim 20).....109
- S. “wherein the server is configured to record video in a tele-medical session mode wherein the blurring the video being transmitted to the destination is not performed when the check determines that the face is not present in the frame” (Claim 13); “wherein the kiosk is configured to record video in a tele-medical

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

	session mode wherein the blurring the video being transmitted to the destination is not performed when the check determines that the face is not present in the frame” (Claim 21)	111
T.	the kiosk ... “provides access to internet web pages via a web proxy, and” (Claim 15h).....	112
U.	“wherein the server is configured to receive a communications request from the device of the outside party and, in response to the received communications request, identify a kiosk in a vicinity of a requested party and transmit a message to the kiosk,” (claim 24); “wherein the server identifies the kiosk in the vicinity of the requesting party by referencing a resident schedule that is stored on a computer readable medium of the server” (Claim 26);	114
V.	“wherein the kiosk is configured to receive the message, and, upon receipt of the message, display an incoming communications request message and initiate a login procedure,” (Claim 24); “wherein the kiosk is configured to receive text-based messages from a server, and to display a notification of an available text-based message on an idle screen of the kiosk” (Claim 8).....	118
W.	“wherein the kiosk is configured to play an alert tone or audio message upon receiving the message.” (Claim 27).....	120
XI.	MOTIVATIONS TO COMBINE THE TEACHINGS OF THE PRIOR ART AND REASONABLE EXPECTATIONS OF SUCCESS.....	120
XII.	DECLARATION.....	128

I. INTRODUCTION

1. I have been retained by the Petitioner, JACS Solutions, Inc., to provide my technical opinions and analysis concerning the validity of the claims of U.S. Patent No. 9,030,292 (the '292 Patent) in light of a combination of prior art provided to me (unless otherwise noted herein) by the Petitioner. I am not an attorney, so my opinions and analysis herein will attempt to refrain from providing legal opinions or conclusions. That said, to the extent that any of my opinions or analyses provided herein are considered to be legal in nature, such opinions or analyses are based upon legal standards provided to me by Petitioner's counsel (and summarized herein).

2. I am being compensated at a rate of \$500 per hour. I have no financial stake or financial interest that depends upon the outcome of this IPR proceeding or on any related activities or matters. This declaration is based on the information currently available to me.

3. In forming my opinions as expressed in this declaration, I have relied on my own knowledge, experience, and expertise, as well as the knowledge of a POSITA (defined below) in the relevant timeframe. The opinions set forth herein are based on my personal knowledge and experience, my professional judgment, and my analysis of the materials and information referenced in this declaration and its exhibits. To the extent that additional information becomes available, I reserve the right to continue my investigation and study, which may include a review of documents and information that may be produced, as well as testimony from depositions that may be taken. I have reviewed and relied upon the following list of materials, and any other cited reference, in this declaration:

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

Exhibit No.	Description ¹
1001	U.S. Patent No. 9,030,292.
1002	Prosecution History for U.S. Patent No. 9,030,292.
1004	Curriculum Vitae of Russell J. Nichols.
1005	First Amended Complaint -- <i>Global Tel*Link Corporation d/b/a ViaPath Technologies v. JACS Solutions, Inc.</i> , No. 23-cv-00500-MN (D. Del. May 22, 2023).
1006	U.S. Patent No. 9,020,114 to Hogg, Jr.
1007	U.S. Patent No. 10,282,563 to Anderson, <i>et al.</i>
1008	U.S. 2010/0299761 to Shapiro.
1009	U.S. 2011/0096139 to Rudolf.
1010	U.S. Patent No. 8,208,000 to Swanson, <i>et al.</i>
1011	U.S. Patent No. 6,665,380 to Cree, <i>et al.</i>
1012	U.S. 2011/0088086 to Swink, <i>et al.</i>
1013	Definition of “kiosk.” Microsoft Computer Dictionary 302 (5th ed. 2002).
1014	“Hands-On: FaceTime for Mac – iPhone videoconferencing app adapted for MacOS X,” Macworld, Jan. 2011.
1015	“Face To Interface – Video-conferencing technology continues to evolve at an astonishing rate, but there are good budget options too. Mark Prigg surveys both ends of the market,” Business Traveler, April 2011.
1016	Summit Schedule and Agenda, Corrections Technology Association, May 23-26, 2010.
1017	“Video Visitation: Evolving Revenue Streams,” Correctional News, May 25, 2010.
1018	Definitions of “biometrics” and “proxy.” Microsoft Computer Dictionary 59-60, 428 (5th ed. 2002).

¹ Descriptions are for convenience only and are not admissions or evidence.

II. TECHNICAL BACKGROUND OF RUSS NICHOLS

4. I am the owner of Russ Nichols Consulting Services, LLC. In addition, I currently serve as a Senior Fellow for the Center for Digital Government, providing advice on policies and best practices in state and local governments. I am also an employee of HiPER Solutions, a company that assists project sponsors and leaders in the execution of their projects. My current CV is attached as Ex. 1004.

5. I earned a Bachelor of Science degree in Computer Science, specializing in Software Engineering, from California State University, Sacramento 1994. I was employed by the State of California from July 1990 until my retirement in November 2022. At the time of my retirement, I was the Deputy CIO (Chief Information Officer) for the State of California.

6. I began my state career with the California Department of Forestry and Fire Protection (“CalFire”) in 1990. Early in my career, I was an email and network administrator for CalFire. In that capacity, I defined the requirements for the email system, then designed and implemented the servers and network infrastructure necessary to support email communications across the state. This included everything from building printer cables to configuring modems and configuration devices. I then moved into a role as a lead software developer for CalFire’s Computer Aided Dispatching system 1993. Because of the system performance requirements, the dispatching solution required system-level coding and complicated conflict resolution practices to ensure that concurrent use by 911 dispatchers would not create resource contention issues as emergency resource capabilities were considered in the context of the 911 calls received in the dispatch center.

7. After several years of software development, in 1995 I moved into leadership roles for CalFire. I managed a collaboration between CalFire and the US

Forest Service to build the Multi-Agency Incident Resource Processing System (“MIRPS”). The MIRPS effort included everything from requirements generation to the development of custom code, testing, and implementation of a system to manage emergency services resources for California and the US Forest Service covering the western states.

8. After several years of software development, in 1997 I moved into leadership roles for the Employment Development Department (“EDD”) and then in 1999, moved back to CalFire. I managed both the software development and infrastructure engineering and support teams. In the management roles, I was responsible for the evaluation, selection, design, implementation, and operation of the entire Departments’ IT networks and both the software and hardware necessary to conduct the Departments’ missions.

9. In 2007 I moved into the role of Technical Operations Chief for the California State Controller’s Office state payroll system. In that position, I was responsible for software design, development, and implementation of an SAP-based Human Capital Management solution. I also worked with data center providers to define the infrastructure necessary to both develop and then operate the solution to support nearly 300,000 California state employees.

10. From January 2010 until March 2021, I worked for the California Department of Corrections and Rehabilitation (“CDCR”). I served as the Director of the Strategic Offender Management System (“SOMS”) from January 2010 to March 2015. SOMS digitized (i.e., computerized) the processes of managing the offender population within the prison system and the parole population in California communities. This included computerized administration of offender demographics, visitor approval processes, disciplinary actions, and offender appeals (complaints). I was directly responsible for the definition of system requirements, solution design, development, testing and implementation of the

solution. In addition to the software system, I was responsible for the design and deployment of the computing infrastructure necessary to implement SOMS. This entailed installing network routers, cabling, and computing equipment in prison housing units and other areas that required strong physical and technical security measures. As a result of these efforts, I received the Administrator of the Year award in 2014.

11. In March 2015, I was appointed by Governor Brown to serve as the Chief Information Officer and Director of Enterprise Information Systems Division for CDCR. In this role, I was responsible for all Information Technology and Telecommunications for CDCR. While in the role, I instituted monthly “vendor days” to provide vendor partners an opportunity to present and discuss their technical solutions with me and my IT management team. This forum facilitated an exchange of technical information and ideas that was often not possible during official procurement processes. This process helped inform vendors of CDCR’s technical landscape and needs, and educated me and the team to allow better, more in-depth technical designs and procurements. During this time, I also sponsored an effort to pilot offender-use kiosks and tablet computers at 5 of CDCR’s 33 prisons, then to expand the program to all prisons. This approach allowed CDCR to document processes for managing tablets and to engage labor unions and regulatory bodies on the usage of offender-based computing devices within the prisons. I also worked with Directors of other Divisions to implement solutions for offender education, digital radio communications, facilities management, and other business needs. I was recognized by Government Technology magazine as Public Sector CIO of the year in 2018.

12. In February 2021, I was appointed by Governor Newsom to serve as Deputy CIO for the State of California. In that position, I was responsible for IT

policy for the state and for the evaluation and approval of automation projects across the 150 departments within the Executive branch of California government.

13. From June 2018 to June 2022, I served as a leader and board member for the Corrections Technology Association (“CTA”), including two years as President. CTA is a public, non-profit network of professionals actively involved in leveraging technology in the corrections industry. Technologies addressed by CTA include offender management systems, health records systems, offender education systems, communication systems, and investigative systems. Offender phone, tablet, and kiosk systems were common topics for the CTA.

14. My experience as a software engineer and technical staff member in addition to my experience as an executive at the CDCR and national leader in Corrections Technology Association combine to make me a unique individual in the corrections industry. My knowledge of prison business operations, security requirements, and the capabilities of different technologies enable me to significantly improve correctional processes and outcomes by safely allowing offender access to technology that had previously been untenable.

15. In addition to my education and professional experience, I served as a member of the United States Marine Corps (reserve) from Mar. 1987 to Dec. 1994. As one of my duties, I was training non-commissioned officer (NCO) for my platoon. For that role, I maintained the platoon’s training and personnel records using an information technology system and I practiced the appropriate security controls necessary to protect the confidential information that reflected battle readiness, and secure records for healthcare and vaccinations.

III. THE ‘292 PATENT

16. The ‘292 Patent is titled “Interactive Audio/Video System and Device for Use in a Secure Facility,” and issued from Application No. 13/088,883, filed on April 18, 2011. Ex. 1001, Cover. The ‘292 Patent describes purported

improvements to “interactive computer systems, and more specifically ... multipurpose interactive audio/video platform ... for use in a secure facility.” *Id.*, 1:6-9. Examples of “secure facilities” provided by the ‘292 patent include “prisons, institutions and other government facilities [that] house large populations of individuals in confinement.” *Id.*, 1:13-15. But the ‘292 Patent also discloses that its applications “could be used in any facility requiring consolidated secure services.” *Id.*, 2:42-45.

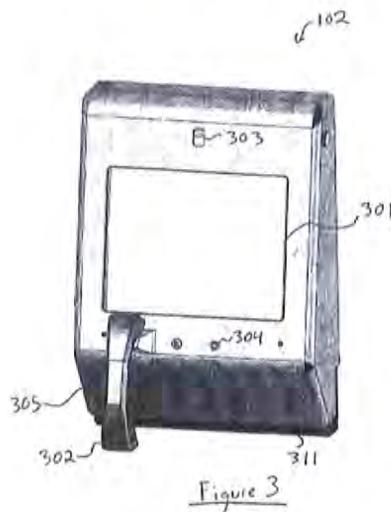
17. The BACKGROUND section of the ‘292 Patent explains that “educational, entertainment, communications, and other services” are provided to individuals in such secure facilities in a “piecemeal” fashion, where “each service [is] handled by different technological means and often even different departments or service providers.” *Id.*, 1:13-27. Further, that “providing these services by a centralized computer system can facilitate more effective monitoring of resident activity.” *Id.*, 1:36-38.

18. The DETAILED DESCRIPTION OF THE INVENTION section thus begins by touting that the patent addresses such problems by providing “a customized interactive audio/video platform for providing administrative services.” This platform includes “kiosks at secure facilities that are interconnected via a central processing platform providing enhanced security and monitoring services,” where the kiosks provide “telephony services, video conferencing, text messaging, tele-medical services, religious and educational services, commissary services, entertainment services, and social networking.” But that these services are “provided in a manner that meets the strict guidelines of a secured facility such as, e.g., a prison.” *Id.*, 2:20-34.

19. The ‘292 Patent does not purport to invent any new type of kiosk. The ‘292 Patent discusses a generic “kiosk with a processor, display, speaker, microphone, and a camera.” (*Id.*, Abstract.) The kiosk may be “a personal

Declaration of Russell J. Nichols in support of petition for *inter partes* review of U.S. Patent No. 9,030,292

computer, a laptop, a mobile device, or a tablet computer device” with a “standard internet browser.” (*Id.*, 8:48–50, 14:19–20.) Or it may be a “touchscreen” with an “optional” “telephone handset” attached:



(*Id.*, Fig. 3., 8:18-43).

20. Nor does the ‘292 Patent purport to invent any new type of central processing system (or any new components of such a system). Indeed, the ‘292 Patent explains, “[e]mbodiments may be implemented using computer hardware or software, or a combination of both. Computer software implementing features of the embodiments may be stored as instructions on a tangible computer readable medium. References to the ‘system’ or ‘platform’ describe specific embodiments and *do not limit the scope of the claimed invention.*” *Id.*, 2:35-41.

21. One administrative service offered through use of the kiosks is video conferencing (also referred to as video visitations) between prisoners and other parties. As part of the video conferencing functionality, the ‘292 Patent discloses the use of generic “facial detection software” to “monitor use of the video conferencing feature.” *Id.*, 14:53-54. The facial detection functionality can be used to monitor the video conference and ensure a face is present in the video; and if

not, blur the transmitted video to “prevent[] inappropriate images from being transmitted.” *Id.*, 14:57-61. The ‘292 Patent does not purport to have invented any video blurring technologies, however. Indeed, the ‘292 Patent doesn’t describe *how* to blur the video at all.

22. Additional uses of the generic facial detection functionality are also disclosed, such as: authenticating a face in the video conference against a face stored in a database (*id.*, 14:62-65); detecting when a second face is present in the video conference (*id.*, 15:6-8); ensuring that only authorized individuals are communicating with a resident during a video conference (*id.* at 15:16-20) and so forth. Despite the stated uses of the generic facial detection software, the ‘292 patent does not purport to have invented any facial detection technologies, nor does the ‘292 patent explain what generic facial detection software one might use for these purposes.

23. Additional purposes for the kiosks are disclosed at a very high level, again without purporting to have invented any technologies associated with these functionalities. These additional functions include voice calling, text messaging, video messaging, telemedical sessions, religious services, educational services, commissary services, and internet access. *See, id.*, 11:37-57.

24. The ‘292 Patent has 29 claims. Claims 1, 15, 22 and 24 are independent.

IV. THE ‘292 PATENT PROSECUTION HISTORY

25. Patent Application No. 13/088,883 was filed on April 18, 2011 with 23 claims. Claim 1 is representative.

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

1. A system for providing services to a secure facility, the system comprising:
 - a kiosk located at a secure facility, the kiosk comprising a processor, display, speaker, microphone, and a camera; and
 - a server that communicates with the kiosk via an internet connection, the server comprising a server processor, a network interface unit, and a computer memory;
 - the kiosk being configured to receive communications from the camera and microphone and transmit audio and video of the communications to the server via the internet connection,
 - wherein the server records the audio and video and transmits the audio and video to a destination, and
 - wherein the kiosk is configured to authenticate the identity of a user of the kiosk by verifying a personal identification number entered by the user and also performing one or more of a facial recognition via the camera and a biometric voice recognition via the microphone.

Ex. 1002, p. 39.

26. As can be seen in the above representative claim 1, it appears to claim a server/kiosk based video conferencing system for “secure facilities” that recorded the video conference on the server and used biometrics to authenticate a user of the kiosk.

27. On Feb. 3, 2012, the Applicants provided some preliminary amendments to the claims. It appears that the purpose of the preliminary amendments was to broaden certain aspects of the claims such as broadening “internet” to “network,” broadening PIN to “log in information” and broadening voice and/or facial recognition to “biometric verification.” *Id.*, pp. 91-99. See amended claim 1 as follows:

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

1. (Currently amended) A system for providing services to a secure facility, the system comprising:

a kiosk located at a secure facility, the kiosk comprising a processor, display, speaker, microphone, and a camera; and

a server that communicates with the kiosk via ~~an internet~~ a network connection, the server comprising a server processor, a network interface unit, and a computer memory;

the kiosk being configured to receive communications from the camera and microphone and transmit audio and video of the communications to the server via the ~~internet~~ network connection,

wherein the server records the audio and video and transmits the audio and video to a destination, and

wherein the kiosk is configured to authenticate the identity of a user of the kiosk by verifying ~~a personal identification number~~ log in information entered by the user and also performing ~~a biometric verification one or more of a facial recognition via the camera and a biometric voice recognition via the microphone.~~

Id., p. 92.

28. On April 26, 2013, the USPTO issued its first Office action, which rejected all claims over the prior art. For example, exemplary claim 1 was rejected as obvious over U.S. Patent No. 8,340,260 to Rae (“Rae”). The examiner stated that Rae disclosed all the claimed elements except for the multi-factor authentication (log-in plus biometric); but then stated that such multi-factor authentication would have been obvious. *Id.*, pp. 108-131.

29. The applicants responded with amended claims and arguments on July 26, 2013. Representative claim 1 was amended to recite the other side of the video call (the “destination” device) and recited that the server authenticates the user of the destination device, as follows:

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

1. (Currently amended) A system for providing services to a secure facility, the system comprising:
 - a kiosk located at a secure facility, the kiosk comprising a processor, display, speaker, microphone, and a camera; and
 - a server that communicates with the kiosk via a network connection, the server comprising a server processor, a network interface unit, and a computer memory;
 - the kiosk being configured to receive communications from the camera and microphone and transmit audio and video of the communications to the server via the network connection[.];
 - wherein the server records the audio and video and transmits the audio and video to a destination; and
 - wherein the kiosk is configured to authenticate the identity of a user of the kiosk by verifying log in information entered by the user and also performing a biometric verification; and
 - wherein the destination is a device communicating with the server, and the server is configured to authenticate a user of the device.

Id., p. 150.

30. The applicants argued that Rae did not teach or suggest a server transmitting the video call to a destination device where the server is configured to authenticate a user of the destination device. *Id.*, p. 157.

31. Another notable amendment was made to independent claim 19. For this claim, the applicants included the following limitation:

wherein the kiosk is configured to detect when a face is not present in the field of view of the camera, warn the user to face the camera if the face is not present in the field of view of the camera and stop transmitting video if the face is still not present.

Id., p. 154.

32. The applicants argued that the combination of Rae and Kenoyer (US 2006/0259755) only disclosed monitoring for a continued presence of a user's face during the video conference, but not terminating the video transmission or warning a user if the face is not detected during this monitoring. *Id.*, p. 163.

Declaration of Russell J. Nichols in support of petition for *inter partes* review of U.S. Patent No. 9,030,292

33. On September 27, 2013, the USPTO issued a final Office action, again rejecting all claims. *Id.*, pp. 168-198. With respect to claim 1, the examiner again cited Rae as disclosing or rendering obvious all claimed elements. *Id.*, pp. 169-171. With respect to claim 19, the examiner stated that Klapman (US 2002/0101512) disclosed warning a user if a face is not present during a video call, and cited that Kenoyer disclosed terminating the video conference transmission if a user is not present in the video call (arguing that Kenoyer's denial of access to the call is analogous to stopping the transmission of video). *Id.*, pp. 187-191.

34. On Dec. 27, 2013, the applicants filed another response in the form of a Request for Continued Examination ("RCE"), amending all independent claims to include the following limitation in some fashion:

wherein the server is configured to periodically extract a frame of the video and perform a check to determine if a face is present in the frame, and the server is further configured to obscure the video being transmitted to the destination when the check determines that the face is not present in the frame; and

Id., pp. 206-217.

35. The applicants argued that none of the combined prior art disclosed this limitation.

36. On March 19, 2014, the USPTO issued another Office action again rejecting all claims. *Id.*, pp. 228-253. In the Office action, the examiner argued that Kenoyer's denying access to the video call if no face is present in the video call was analogous to obscuring the transmission of video as claimed. *Id.*, p. 233.

37. On June 19, 2014, the applicants amended the claims again. *Id.*, 258-269. Exemplary claim 1 is representative:

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

wherein, after the user identity has been authenticated by the kiosk and during the transmission of the video, the server is configured to periodically extract a frame of the video and perform a check to determine if a face is present in the frame, and the server is further configured to blur or obscure the video being transmitted to the destination when the check determines that the face is not present in the frame; and

38. The applicants then attempted to distinguish Kenoyer's authentication activities from the claimed video obscuring or blurring.

Kenoyer, however, neither discloses nor suggests blurring or obscuring a video transmission where a face is not present in a frame thereof, as recited in claims 1 and 22. Kenoyer, at most, discloses that a face detect module 404 and face match module 406 could be used to authorize a user attempting to log in to a system. Kenoyer, at ¶¶ [0041]-[0044]. Unlike the system and method of claims 1 and 22, Kenoyer does not disclose a system where *a video being transmitted, after user authorization*, is checked to determine whether a face is present. Kenoyer also fails to disclose a system where a video being transmitted is blurred or obscured where there is no face present in a frame extracted from the video.

Id., p. 266.

39. On July 24, 2014, the USPTO issued another final Office action again rejecting all claims. *Id.*, 273-301.

40. With respect to the amended limitation and arguments, the Examiner argued that Kenoyer still disclosed this limitation:

Regarding Applicant's arguments that the references do not disclose the amended subject matter on pages 9-12, the Examiner respectfully disagrees. The claim limitations specifically say that the check is to "determine if a face is present in the frame" and then obscuring the video "when the check determines that *the* face is not present in the frame." That is, the video is obscured if the face that was initially present

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

is not present in the subsequent frame. Kenoyer discloses an initial biometric authentication of a user in paragraphs [0041]-[0042], where the user is authenticated in order to log in to the videoconference network. This is analogous to the limitation "after the user identity has been authenticated by the kiosk". Kenoyer further goes on to say that the user is continuously authenticated to ensure that the user in front of the videoconference system continues to be the same authenticated user at all times, paragraph [0044]. This would apply, then, to during the actual video conference, where video is being transmitted to other participants of the video conference, as discussed in paragraph [0046] where the user joins a video conference in progress. In cases where the user is not authenticated, the user is denied access to the videoconference network, paragraph [0042]. It is obvious to one of ordinary skill in the art that the denial of access is applied in all cases where a user is not authenticated, including during a video conference that is in progress.

So, during the continuous authentication disclosed by Kenoyer, it is plausible that during a first authentication, the user is the same and is thus authenticated. This is analogous to the limitation "configured to periodically extract a frame of video and perform a check to determine if a face is present in the frame." In this case, the user would be allowed to remain in the video conference that is in progress. However, in the continuous authentication of Kenoyer, it is also plausible that the user may switch with a second user that is not authenticated. In Kenoyer's system, the second user that is not authenticated would not have the same face as the authenticated user, and the second user would be denied access to the videoconference system. This is analogous to the limitation "configured to obscure the video being transmitted to the destination when the check determines that *the* face is not present in the frame." Because the same face is not present in the frame, the user may no longer access the video conference network, and the video associated with that particular user would no longer be transmitted to other participants of the video conference. The limitation in the claim states that the video is blurred or obscured, in the alternative. Therefore, the claim does not require the reference to disclose both blurring and obscuring the video. As such, Kenoyer discloses the amended subject matter required by the claim.

Id., pp. 298-300.

41. On January 26, 2015, the applicants filed another RCE to amend the subject limitations to specify that the specific type of obscuring that is occurring is blurring. *Id.*, pp. 304-316. The amendment to claim 1 is representative:

wherein, after the user identity has been authenticated by the kiosk and during the transmission of the video, the server is configured to periodically extract a frame of the video and perform a check to determine if a face is present in the frame, and the server is further configured to blur or-obscure the video being transmitted to the destination when the check determines that the face is not present in the frame; and

Id., p. 305.

42. The applicants argued that “blurring” is different than the termination of the call (i.e., “obscuring”) disclosed by Kenoyer. *Id.*, p. 313.

43. In response, on March 20, 2015, the USPTO issued a Notice of Allowance. *Id.*, 322-328. The following is the examiner’s “Reasons for Allowance”:

The prior art of record does not disclose, nor is there motivation to combine, a system for providing video services to a secure facility that periodically authenticates a user of a kiosk in the facility by performing biometric authentication of the video after an initial authentication, and blurs the video being transmitted when it is determined that a face is not present in the frame.

Id., p. 327.

44. On April 3, 2015, the applicants filed another amendment to correct a typographical error in dependent claim 27. *Id.*, pp. 348-356. This amendment was entered by the USPTO on April 15, 2015. *Id.*, pp. 363-364.

45. Finally, on May 12, 2015, the application issued as U.S. Pat. No. 9,030,292.

V. THE PRIORITY DATE OF THE '292 PATENT AND THE STATE-OF-THE-ART AT THAT TIME

46. I have been informed that the “priority date” for the ‘292 Patent is April 18, 2011.

47. I understand and recall that, generally, video calls and video conferencing using computing devices was an established technology and product as of the priority date of the ‘292 patent. *See, e.g.,* (<https://www.techtarget.com/whatis/feature/The-history-and-evolution-of-video-conferencing>).

48. In 2010, public use of video conferencing exploded with the introduction of the Apple iPhone 4 and the Facetime application. *See, e.g.,* Ex. 1014. In addition, similar products like Skype and Webex were widely used as of the priority date of the ‘292 Patent. *See, e.g.,* Ex. 1015.

49. In the 1990s, many organizations began using Polycom or similar products to support conference calls involving multiple parties. That functionality quickly evolved into video conferencing solutions, with Skype introduced in the early 2000s. The number of registered users of Skype was about 50 million in 2005 and increased more than 10-fold to more than 600 million just five years later. *See, e.g.,* (<https://www.britannica.com/technology/Skype>).

50. Because correctional organizations are often located across multiple geographic locations, audio and video conferencing solutions were utilized to connect staff and eliminate the need for extensive travel. That functionality also became a topic of interest to reduce the risk imposed by moving offenders between facilities, courts, or even in communication within facilities.

51. Based upon my experience working with corrections facilities and my association with correctional groups across the country, communication between offenders and people outside of correctional facilities introduces risk that must be

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

managed to ensure the safety of both staff and offenders. Communication that is not in-person (such as phone calls, mail, electronic messages and video visits) is tightly controlled and monitored, with the exception of protected instances (e.g. communication with their attorney). Even when the communication is managed, a lot of illegal activity is conducted from inside the prison. It is common in California, and many other jurisdictions as well, for gang activity to be managed and directed from inside the prison system by incarcerated gang leaders. Activities include escape plans, drug deals, and witness intimidation, for example.

52. As a result, correctional institutions have traditionally taken a hyper-conservative approach to electronic communications involving prisoners. Correctional institutions have been very slow to adopt such electronic communications and have operated under the “prove to me that nothing bad can happen before we will bring this in” type of mentality.

53. In my experience, adoption of such electronic communications occurred more quickly in Europe, but has since been growing in the United States. In the last decade, many correctional organizations in the United States have looked at some of the European models, specifically the Scandinavian models, on how to make the prison setting a more rehabilitative environment rather than just a punitive environment. The models differ in approach. Generally, in the US, new prisoners are afforded few privileges and are required to earn increases in privileges (such as access to electronics and electronic communications) going forward. In other models, it has generally been the opposite – new prisoners initially have many privileges, which then may be lost due to bad behavior. The comparative studies and data analytics between these two models seem to indicate that outcomes may be better using the European model. The European model is also considered more humanistic. With a focus on correctional reform and rehabilitation, I believe US

jurisdictions have increased access to electronic devices and communications in US correctional facilities over the last decade.

54. With that background, the '292 patent is presenting a video visitation system and an associated kiosk in the April 2011 time frame. And the patent discloses that a tablet computer could be used as the kiosk – you just take a tablet computer and that becomes your kiosk (typically encased in a protective case or box in my experience, but the '292 Patent does not require that). As of the April 2011 time frame, I recall there were a number of jurisdictions looking at remote video type visitations sessions. This is especially true in jurisdictions with challenged staffing levels. Managing an in-person visitation process is staff intensive. Every visitor that comes in needs to be validated to ensure they are a legitimate visitor and searched to ensure safety of the staff and offenders present. Consequently, there is a lot of overhead.

55. There are many risks with in-person visitations. Risk range from the introduction of contraband to the introduction of contagions. As a result, visitation can be shut down because of an illness, injury, or a security concern in the prison or in the outside population.

56. Consequently, during the April 2011 timeframe there were many organizations looking for a way to conduct visitation without many of the risks of in-person visitations. And, as a result, many organizations were looking at having video visitations as a potential solution. For example, during the 2010 Corrections Technology Association summit, when the prison system CIOs and technology representatives come together about the topics that are in the prison, there were two sessions specifically directed to remote video communications. *See*, Ex. 1016. I also found a May 2010 article out of Correctional News about video visitations in prisons. *See*, Ex. 1017. This article discussed reasons to have video visitations in prisons and also discussed the evolving revenue streams associated with that.

57. During this same timeframe it was also common for prisoners to be able to purchase items from prison commissaries. Due to security concerns, we could rarely have a simple store where prisoners could pull items off the shelf. We typically had to set up various solutions such as providing a paper notepad in which prisoners could simply check off the available items they wished to purchase. There was always some sort of request-fulfillment process involved. And the '292 patent merely discusses automating that process by adding the automated request-fulfillment process to the same kiosk device that offers video communications. The '292 patent does not really discuss anything concerning the materials management, warehousing or procurement processes because all of that is handled separately.

VI. THE LEVEL OF ORDINARY SKILL IN THE ART FOR THE '292 PATENT

58. The '292 Patent is primarily directed to "interactive computer systems, and more specifically to providing a multipurpose interactive audio/video platform and device for use in a secure facility." 1:6-10.

59. I have been informed and understand that a person of ordinary skill in the art ("POSITA") is a hypothetical person who is presumed to have known the relevant art at the time of the alleged invention. Based upon my understanding of the '292 Patent specification and claims, it is my opinion that the relevant Field of Technology or ("art") with respect to the '292 Patent is Information Technology (IT), or more specifically, Computer Science or Computer Engineering as applied in a correctional institution (or a facility having similar security concerns such as hospitals, law enforcement offices, military facilities, and the like).

60. I have been informed and understand that the disclosure of patents and prior art references are to be viewed from the perspective of a person having ordinary skill in the art at the time of the alleged invention. I provide my opinion

from the viewpoint of a person having ordinary skill in the art as of the earliest
alleged priority date for the '292 patent.

61. I have been informed that the following five factors inform the analysis
for determining the level of ordinary skill in the art: (1) type of problems
encountered in the art; (2) prior art solutions to those problems; (3) rapidity with
which innovations are made; (4) sophistication of the technology; and
(5) educational level of active workers in the field. *In re GPAC Inc.*, 57 F.3d 1573,
1579 (Fed. Cir. 1995). I apply these factors in the paragraphs below in providing
my opinion as to the level of one having ordinary skill in the art with respect to the
'292 Patent.

62. With respect to (1), there are many things that need to be considered
with respect to video conferencing in correctional facilities. One problem is that
you need to be able to control what is shown on the screen during the video call.
For example, you generally don't want the video conference to show what is in the
background of the prisoner (don't want to show prison staff on the screen for
example); you don't want any nudity; you don't want messages being passed (the
prisoner could seem to be having a normal conversation but sending messages
through sign language or holding up notes and the like). These were all common
concerns as of the April 2011 timeframe.

63. With respect to (2), there were several vendors as of the April 2011
timeframe offering IT solutions for correctional institutions. *See, e.g.*, Ex. 1016 and
Ex. 1017. These vendors included JPay and Keefe Group. Most of these vendors
utilized off-the-shelf technologies but with customized software and hardened
cases to address the needs and security concerns surrounding correctional facilities.
With respect to video visitation technologies, the vendors would typically set up
the visitation kiosks in a room where there was little risk of what was in the

background or overhearing other conversations, essentially using many of the long-standing practices for in-person visitations such as physical barriers.

64. With respect to (3), as I discussed above many jurisdictions were slow to adopt these new technologies, but not due to technological limitations. Most slow adopters were simply very risk averse or set in their ways. Some jurisdictions, though, were quick to adopt for other reasons, such as lack of manpower to run in-person visitations. In those cases, the computing devices themselves didn't change – the kiosks essentially implemented whatever off-the-shelf tablet devices or the like that were available at the time. As far as I am aware, nobody was designing custom chip-sets for use in correctional facilities, for example. As I said above, the solutions I was aware of were custom programmed products using off-the-shelf technologies for the most part. The '292 Patent, for example, does not provide any new computing technologies or devices. Nor does the '292 Patent provide any new or specific software algorithms for facial recognition, user authentication, video conferencing or the like.

65. With respect to (4), the sophistication of the technology involves understanding the needs and security concerns for using IT in correctional facilities and implementing/programming off-the-shelf technologies to address these needs and concerns. It certainly took some level of IT education and experience, in addition to real knowledge of these needs and security concerns to put all the components together and make them work.

66. With respect to (5), the current job specification for IT staff in California prisons is a reasonable example of the education and experience levels that correctional institutions were looking for in April 2011. *See*, CA IT series classifications (<https://www.calhr.ca.gov/state-hr-professionals/pages/1400.aspx>). Not all jurisdictions would have the resources of California, so others may have more flexible requirements. That said, in my experience, the California listing is

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

consistent with minimum levels of skill that I would expect someone to have when designing the types of solutions provided in the '292 Patent.

67. Based on this understanding, it is my opinion that a POSITA with respect to the '292 Patent will have 120 semester units or 180 quarter units (essentially a Bachelor's degree) from an accredited college or university including at least 15 semester units (or 22.5 quarter units) of information technology or closely related course work; or, without such education, will have four years of general information technology experience performing technical and/or analytical tasks for computer systems or services in any of the six domains or emerging information technology fields (Business Technology Management, Client Services, Information Security Engineering, Information Technology Project Management, Software Engineering, and System Engineering). *See, e.g.*, CA IT series classifications (<https://www.calhr.ca.gov/state-hr-professionals/pages/1400.aspx>). In addition, any substantially equivalent combination of experience and education should suffice.

68. In addition to the education and general information technology assistance experience discussed above in ¶67, a POSITA will also have at least 12 months working with IT in a prison, jail, associated jurisdictional organization, hospital, military facility, law enforcement facility (or similar secure facility that houses residents in a secure manner). The more direct experience that involves resident (offender) IT security the better. Additional education may substitute for some of the of the experience to the extent that such additional education focuses on secure IT systems. Likewise, certain direct experience may substitute for some education.

69. Due to the moderate design and implementation complexities in the field, a POSITA with respect to the '292 Patent will have an above-average-level of risk assessment and problem-solving acumen and would seek various available

solutions to offender IT services problems (as shown in Ex. 1016 and Ex. 1017, many correctional facility IT services vendors were available as of the '292 Patent priority date). But such POSITA would not be restricted to looking at IT service solutions for correctional facilities. A POSITA would look to other areas of information technology communications and solutions design (such as, for example, medical privacy management, military security management, law enforcement data security management, etc.) to find similar solutions to similar problems confronted in the correctional institution IT field. Id. ¶38.

70. Based on my education and professional experience, I believe that I qualify as understanding and possessing the knowledge and skills of a POSITA as of the April 18, 2011 time period, and I have a sufficient level of knowledge, experience, and expertise to provide an expert opinion in the technology field of the '292 Patent. I have used my education and experience as described above, as well as my understanding of the knowledge, creativity, and experience of a person having ordinary skill in the art (POSITA) as of April 18, 2011, in forming the opinions expressed in this report, as well as any other materials discussed herein. Any time I refer to a POSITA in this declaration, I am referring to the time frame of prior to and up to April 18, 2011. Unless otherwise stated, my opinions set forth herein are as a POSITA as of the April 18, 2011 timeframe.

71. If the PTAB adopts a different definition for a POSITA that is at least somewhat consistent with my definition, my opinions set forth herein would not change. If the PTAB (Patent Trial and Appeal Board) adopts a definition that is remarkably different than my definition then I would need to consider that markedly different definition, but I do not think it would change my opinions set forth herein.

VII. CLAIM INTERPRETATION

A. The Principles of Patent Claim Interpretation (Also Known as Claim Construction)

72. I am not an attorney. For the purpose of this report, I have been informed about certain aspects of the law that are relevant to my analysis and opinions as presented herein.

73. I understand that *inter partes* review (“IPR”) is a proceeding before the United States Patent & Trademark Office (“USPTO”) for evaluating the validity of issued patent claims. I understand that, in this *inter partes* review, a claim term is construed as it would have been understood by a POSITA in view of the patent’s specification and prosecution history. I understand that the “specification” of a patent includes all the figures, discussion, and claims within the patent. I understand that the USPTO will look to the specification and prosecution history to see if there is a special definition for a given claim term, and if not, will apply the plain-and-ordinary understanding of the term according to a POSITA at the time in which the alleged invention was made. I also understand that this plain-and-ordinary definition must be made in light of the patent specification. For example, the plain-and-ordinary meaning of the term cannot be inconsistent with how the term is used in the patent specification.

74. I understand that the specification and prosecution of history of the patent is considered to be the “intrinsic record,” while materials and information outside of this intrinsic record are considered “extrinsic evidence.” Further, I understand that it is improper to rely to the extrinsic evidence for determining the meaning of a claim term if the intrinsic record is clear. That said, I also understand that certain extrinsic evidence (such as dictionaries, treatises and such) may be considered to help understand the plain-and-ordinary meaning of certain terms if the intrinsic record is not so clear on that point.

B. Interpreting Certain Claim Limitations from the ‘292 Patent

1. Secure Facility

75. The ‘292 Patent does not define secure facilities but explains that “secure facilities *require additional levels of monitoring and oversight that are not required when similar services provided to other populations.*” Ex. 1001, 1:18-21. Examples of secure facilities include “prisons, institutions, and other government facilities house large populations of individuals in confinement.” *Id.*, 1:13-16. But the ‘292 Patent also does not limit the term to prisons and such by saying that “[t]hough embodiments are described with reference to facilities such as prisons or detention facilities, the embodiments described herein could be used in *any* facility *requiring consolidated secure services.*” 2:42-45. As such, the appropriate construction is *a facility that requires levels of monitoring or oversight that are not generally required for populations outside of the facility.*

2. Kiosk

76. A dictionary definition of “kiosk” is a “a freestanding computer or terminal that provides information to the public, usually through a multimedia display.” (See, Ex. 1013, Microsoft Computer Dictionary Fifth Edition 2002). I generally agree that this is an accurate definition outside of the correctional institution context. Within a correctional institution context, the kiosk is typically a computing device (such as a desktop, tablet or laptop computer) encased in a hardened (tamper-proof) housing and installed on the wall, in a room or on some sort of rolling unit. That said, the ‘292 Patent expressly broadens the term to include “*a standalone structure, a personal computer, a laptop, a mobile device, or a tablet computer device.*” Ex. 1001, 8:47-50. For the purposes of this report, I have adopted the broadened definition provided by the ‘292 Patent.

3. Biometric Verification

77. The '292 Patent does not define "biometric verification," but provides two examples: voice recognition (Ex. 1001, Abstract, Claim 11) and face recognition (Ex. 1001, Claim 10).

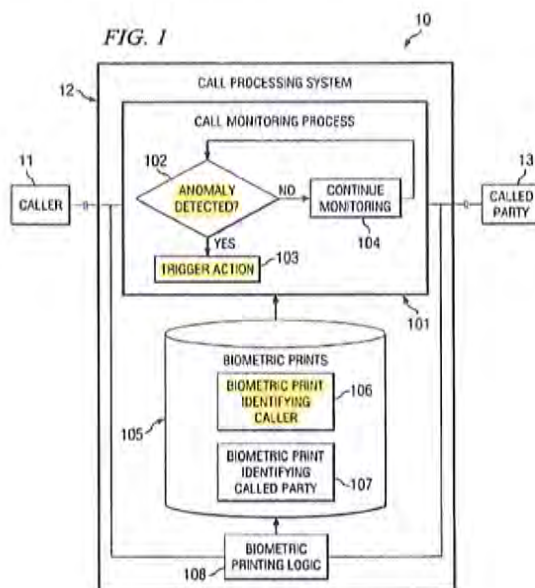
78. "Biometrics" is defined by the Microsoft Computer Dictionary as the "science of measuring and analyzing human biological characteristics." Ex. 1018. The definition continues, "[i]n computer technology, biometrics relates to authentication and security techniques that rely on measurable, individual biological stamps to recognize or verify an individual's identity. For example, fingerprints, handprints, or voice-recognition might be used to enable access to a computer..." This definition is consistent to how "biometric verification" is used in the '292 Patent. As such an appropriate construction would have been "*verification via biological phenomena, such as voice or face recognition.*"

VIII. THE PRIOR ART

A. Hogg

79. Hogg was not considered during prosecution of the '292 Patent. Hogg is directed to the use of biometric identification (e.g., facial identification or voice recognition) for detecting anomalies during calls, such as video calls, in correctional facilities. "*Embodiments of the present invention are directed generally to use of biometric identification during a call for detecting an anomaly occurring in the call, such as a change in the parties participating on the call. ... [C]ommunication between parties of a call is monitored and biometric identification is performed using the communication. ... The call is then monitored and video communication of the call (e.g., of a video conference call) is used for comparison with the face prints to detect changes in the parties participating on the call, such as a new, unauthorized party joining the call. Thus, embodiments of the present invention advantageously enable a call processing system to monitor*

calls and detect anomalies occurring during the calls, such as three-way calling, a handoff of a call from one party to another, etc.” Ex. 1006, 4:44-55.



Ex. 1006, Fig. 1.

80. Hogg disclosure is specifically applicable to correctional facilities or other controlled environments. “Embodiments of the present invention have *particular applicability within controlled-environment facilities* for monitoring the calling activities between a resident and other parties. Examples of controlled-environment facilities include *correctional facilities ... healthcare facilities ...*, restricted living quarters ... and the like.... [T]he concepts disclosed herein may likewise be employed in other environments.” *Id.* 4:66 to 5:28.

81. Hogg recognizes that “[i]n many environments, monitoring of telephony calls to detect and/or prevent unauthorized activities is desirable. For example, private premise-based telephone systems, such as those installed at correctional facilities or other controlled-environment facilities, generally desire to monitor various events occurring on the telephone lines of the system.” *Id.*, 1:45-50. Hogg also recognizes, that “to preserve this screening activity, it is often desirable to

insure that the called party is in fact the person to whom the call is terminating. Therefore, it is often desirable to have control of the call with respect to all the parties who are on the phone call. In short, it is desirable to prevent addition of an unknown third party to a resident call in order to preserve the integrity of the initial call screening.” *Id.* 2:11-18.

82. Hogg discloses that pre-authenticated video call users/callers have facial recognition performed on video “prints” (e.g., frames) during the video calls to check if the expected face is present in the print/frame to monitor, for example, for any changes in the parties participating in the video call. *Id.*, 4:55-65, 10:6-14. And *if the expected face is not detected, Hogg discloses taking protective action for the video call such as recording the call, notifying appropriate personnel, or terminating the call.* *Id.*, 9:26-44.

B. Anderson

83. Anderson was not considered during prosecution of the ‘292 Patent. Anderson describes “applications in the areas of data processing, portable computing, *computer-based communications, computer security*, and data privacy maintenance.” Ex. 1007, 1:28-36. In particular, Anderson “*provides for privacy protection in portable computing devices that incorporate displays.*” *Id.*, 4:28-33. Anderson expressly discusses use in secure environments and facilities: “computer users can view data on a computer-controlled display *in a variety of secure and unsecured environments* with greater security from unwanted and undetected eavesdropping and tampering”, such as found “commonly in *government, scientific, engineering, and military applications...*” *Id.*, 4:28-37, 9:20-38.

84. Anderson recognizes that off-the shelf computing devices, such as laptop computers, PDAs and tablet computers “cannot adequately maintain privacy for information displayed to the user while the device is in use.” *Id.*, 1:40-46. As an example, Anderson discloses a need for security intervention in video calls: “*if a*

user is on a Skype conference call, and someone enters their office and discloses sensitive information, others on the call may overhear it. Some means to automatically mute the microphone when the user shifts attention from the computer, such as to look at someone entering their office, is needed to reduce the chance that verbal information will be inadvertently disclosed.” Id., 3:46-52.

85. To resolve these security issues, Anderson discloses that it provides “systems, software, and methods to maintain privacy of displayed data by using sensor-derived information about the user or other authorized individuals, ... to detect, and optionally to identify, the user, optionally authorize device use ..., detect and notify the user of unauthorized viewers ..., inhibit unauthorized viewers, and to reduce the amount of displayed information available to unauthorized persons or devices. The sensor-derived information is also used, in some embodiments, to ... to record or transmit information (or both) about the device location, environment and person or persons in the vicinity of the device. These capabilities are, in some exemplary embodiments, implemented in such a way as to support centralized security policies and enforcement of these, with audit data maintained to permit later analysis of adherence to them.” *Id.*, 7:50 to 8:1.

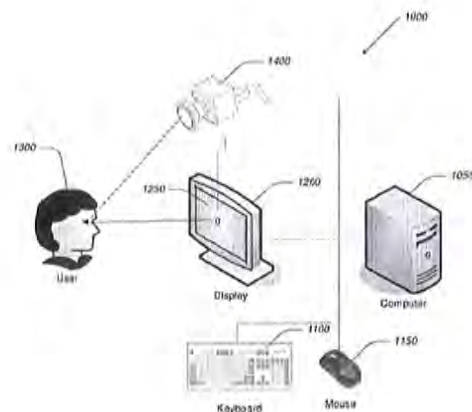
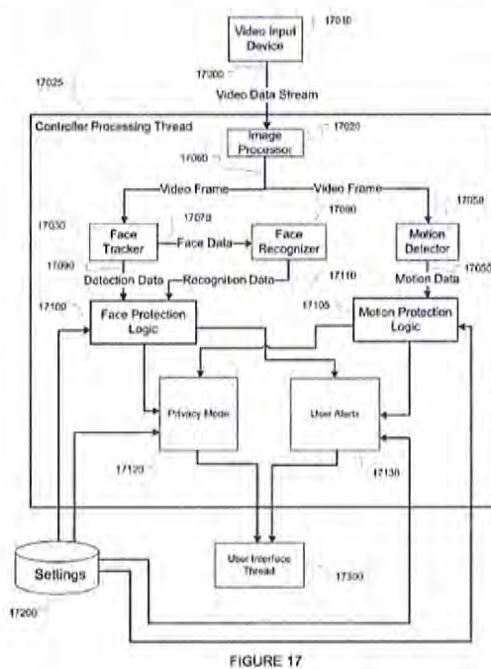


FIGURE 1

Ex. 1007, Fig. 1.

86. Anderson discloses using kiosks (e.g., “portable computing devices that incorporate display,” such as a “tablet-based portable computer”, a “PDA”, a “desktop computer” or a “laptop or notebook computer”) to perform video conferences. *Id.*, 4:28-59, 8:44-62, 16:14-39, 21:52-61. Anderson discloses that, during the transmission of video, the security software periodically extracts a frame of video and performs a check to determine if the user’s face is present in the frame. *Id.*, 4:38-56, 6:14-43, 11:21-25, 12:39-43, 13:41-43, 16:10-39, 18:33-37 and 30:62-31:19. The absence of the user’s face in the video is disclosed by Anderson as one of the possible triggers for “privacy mode.” *Id.*



Ex. 1007, Fig. 17.

87. Anderson discloses that in privacy mode (which may be activated when a user’s face is not detected by the facial recognition tracker) the video from the webcam (i.e., video input device) may be obscured. *Id.*, 16:14-39. Further, Anderson also discloses that one type of video obscuring is blurring. *Id.*, 16:40-52, 35:13-55.

88. One example of Anderson's technology is what may happen during a video conference call, "for example when a user is distracted from a video conference by a supervisor entering their office." Anderson explains, "[a]s *the user looks away from the display device, others on the video conference call are not enabled to overhear or see the discussion between the user and the user's supervisor. When the user looks back to the display device to continue the video conference, the diversion or blockage of the web camera data is halted and normal video input resumed, and the microphone is un-muted.* By controlling device input and output in this manner, all applications that make use of these devices effectively gain increased privacy control features, without requiring that any of these applications, such as *video conferencing*, Voice over Internet Protocol ("VoIP"), MP3 players, or others, be modified in any way. Instituting the foregoing can be done by those having ordinary skill in the art using the disclosure and drawings herein." 26:50-67.

C. Shapiro

89. Shapiro was not considered during prosecution of the '292 Patent. Shapiro is directed to a kiosk-based platform for a correctional facility that monitors prisoners' electronic messages. "The invention includes delivering and monitoring electronic letters to correction facility inmates while giving supervisory authorities the ability to screen the incoming mail." Ex. 1008, Abstract, [0007]. Shapiro also discloses that the same kiosks may also be configured to provide the prisoners access to electronic media along with access to the electronic messages. "Another aspect of the invention involves providing a computer-operated kiosk that may be used by individuals (e.g., inmates) in a restrained environment/restricted-access location (e.g., a prison) to browse through a catalog of available digital media... The digital content player device may also be used to display correspondence to inmates." *Id.*, [0008].

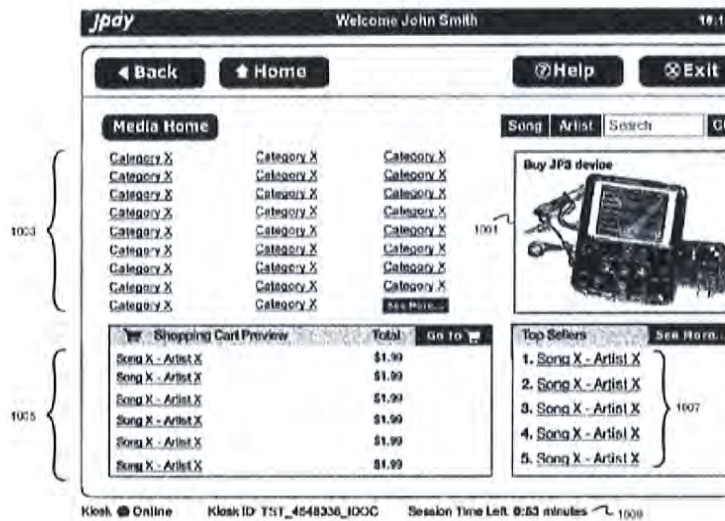


Fig. 10

Ex. 1008, Fig. 10.

90. Shapiro discloses a server (such as a local server) that communicates with the kiosks via a secure network connection; and that the server includes standard server/computer components such as a system bus 221, a server processor (processing unit 220), a network interface unit (network interface 170) and a computer memory (System Memory including ROM 231 and RAM 232). *Id.*, [0022], [0133].

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

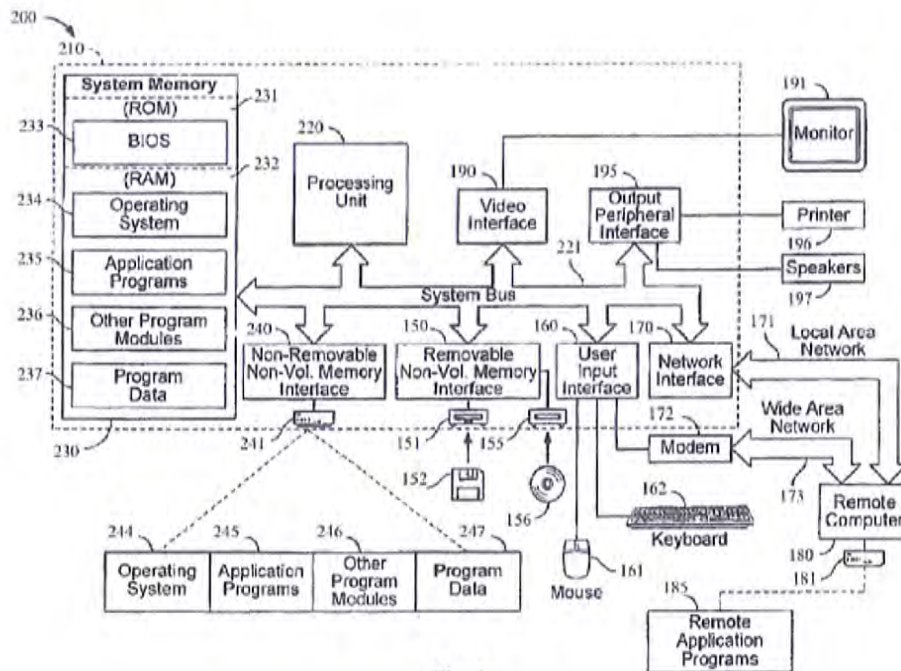


Fig. 1

Ex. 1008, Fig. 1.

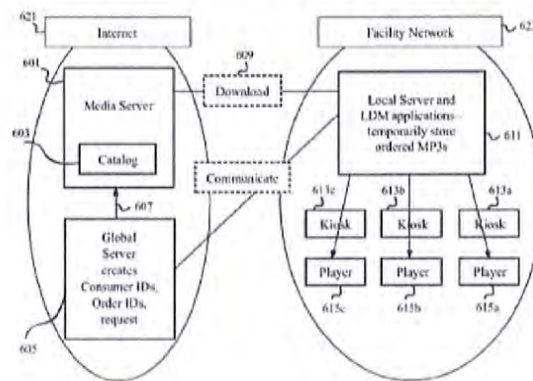


Fig. 6

Ex. 1008, Fig. 6.

D. Rudolf

91. Rudolf was not considered during prosecution of the '292 Patent. Rudolf is directed to a kiosk-based video visitation system for a prison that provides for

recording the video visitations and inmate messaging. Ex. 1009, [0001], [1007], [1008]. “This invention relates generally to systems and methods for implementing video visitation where the only contact between individuals is through a video and audio connection.” *Id.*, [0001]. “The present invention is also applicable to systems including a network video recorder and wherein transmitting the combined audio/video signal to the communication station identified in the received communication station includes transmitting the signal to the network video recorder. The present invention is also applicable to systems wherein communication timing is managed by an administration system, which is configured to transmit timing messages to the communication stations.” *Id.*, [0008].



Fig. 3C
Ex. 1009, Fig. 3C.

92. Rudolf recognizes that “[v]ideo visitation communication systems allow communication between two communication stations using audio and video devices. These systems may be used in a correctional facility to allow family and friends to visit with inmates while keeping direct contact to a minimum. Advantageously, the individuals communicating may be separately located such that no direct interaction occurs.” *Id.*, [0002]. Rudolf also recognizes that

“[p]roviding connections between communication stations needs to be simple and quickly completed to allow guards to easily manage visitation.” *Id.*, [0003].

According to Rudolf, “[o]ne skilled in the art will appreciate that the present invention realizes a number of advantages over video visitation systems of the prior art. One such advantage is that the present invention provides for quick and easy communication channel management. In this regard, the present invention may be particularly advantageous for minimizing visitation overhead, training, etc. for the correctional officers of a facility.” *Id.*, [0049].

E. Swink

93. Swink was cited by the examiner during prosecution of the ‘292 Patent (but was not cited in combinations with Hogg, Anderson or Shapiro). Swink is directed to technologies for securing an electronics communication device such as a mobile phone. Ex. 1012, par [0005]. Swink discloses displaying a notice of an incoming message on a display screen of a kiosk (mobile device). *Id.*, [0015].

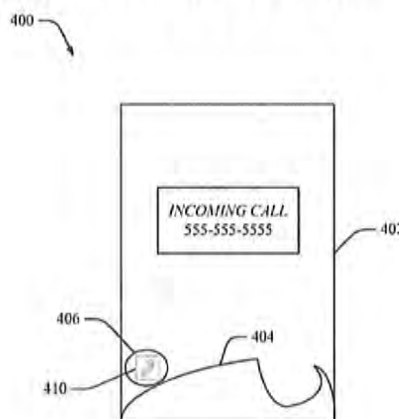


FIG. 4

Ex. 1012, Fig. 4.

F. Cree

94. Cree was cited by the examiner during prosecution of the '292 Patent (but was not cited in combinations with Hogg, Anderson or Shapiro). Cree is directed to a telecommunications system for prisons that alerts inmates for messages from parties outside of the prison facility and monitors and tracks the messages between the prisoner and outside parties for security purposes. "The invention relates to the *field of telecommunications* and, more particularly, to an *inmate messaging system and method for notifying an inmate in a prison facility of messages received from a caller outside the prison facility.*" Ex. 1011, 1:6-9. "Still another advantage of the present invention is the *ability to track messages between remote callers and inmates for both billing and security purposes.*" *Id.*, 3:7-13.

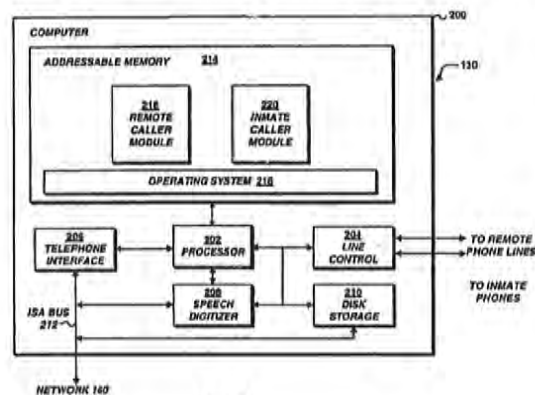


FIG. 2A

Ex. 1011, Fig. 2A.

95. Cree recognized the "need within the inmate telephone industry to facilitate notification of inmates when a remote party desires to communicate with an inmate via the inmate telephone system." *Id.*, 1:33-37. So, in addition to tracking messages with inmates, Cree also provides that "inmates in a prison facility can be notified of pending messages in an efficient and economical manner." *Id.*, 2:64-66. And, further, that "all messaging functions are properly

controlled by the messaging system to prevent their exploitation by inmates.” *Id.*, 3:4-6.

96. Cree also discloses that its inmate messaging system delivers a message from an outside party to a prisoner by automatically dialing the kiosk in the cell block the prisoner is located; and also delivers a notification to the inmate that a message is available (i.e., list of pending messages). *Id.*, Abstract, 10:19-22, 10:51-53.

G. Swanson

97. Swanson was not cited during prosecution of the ‘292 Patent. Swanson discloses server-based technologies for managing video conferences. Ex. 1010, Abstract. Specifically, Swanson discloses managing video conferencing between Users 1-75 over a network 110 by a video conference server 112. *Id.*, 10:36 to 11:9.

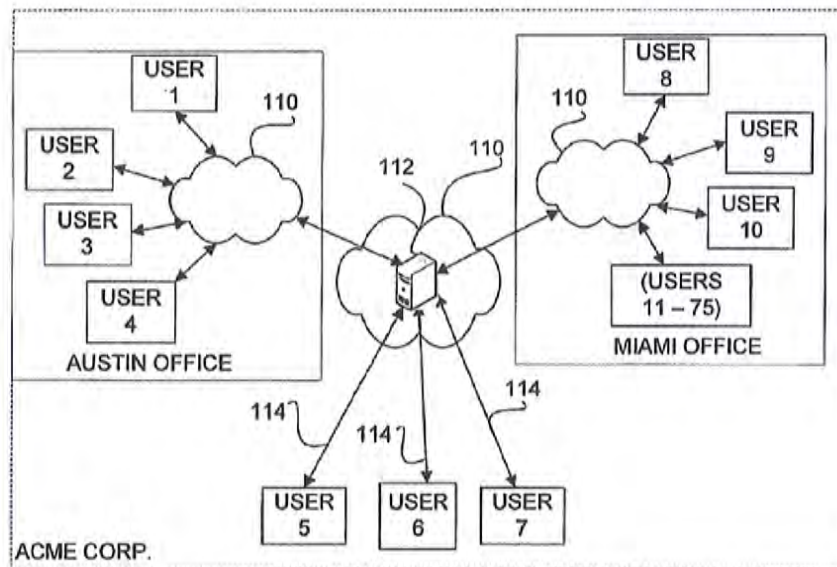


FIG. 4

Ex. 1010, Fig. 4.

IX. THE PRINCIPLES AND LAW OF PATENT INVALIDITY

98. I am not an attorney. For the purpose of this report, I have been informed about certain aspects of the law that are relevant to my analysis and opinions as presented herein.

99. Invalidity by Anticipation: I understand that a patent is invalid as anticipated only if each and every element and limitation of that claim is publicly disclosed—either expressly or inherently—in a single prior art reference. I understand that such anticipation requires the presence in a single prior art disclosure of all elements of the claim arranged as in the claim. I further understand that for a step or limitation to be inherent in a reference, the step or limitation must necessarily and inevitably occur or be present when one follows the teachings of the reference.

100. Invalidity by Obviousness: I understand that a patent claim may be unpatentable if the claimed invention would have been obvious to persons having ordinary skill in the art in the field of the technology of the patent at the time the invention was made. A claim that would have been obvious may be unpatentable even if all the requirements cannot be found in a single prior-art reference.

101. I understand that obviousness is analyzed from the perspective of a hypothetical person of ordinary skill in the art (“POSITA”) at the time of the alleged invention. I also understand that a POSITA is presumed to have been aware of and be able to understand the disclosures of all pertinent prior art at the time of the alleged invention.

102. As part of this inquiry, I understand and have considered the level of ordinary skill in the art that someone would have had at the time of the invention. To determine the level of ordinary skill, I have considered the levels of education and experience of persons working in the field; the types of problems encountered in the field; and the sophistication of the technology.

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

103. I understand that an obviousness analysis involves comparing a claim to the prior art to determine whether the claimed invention as a whole would have been obvious to a POSITA in view of the prior art, and in light of the general knowledge in the art at the time the invention was made. I also understand that the claim would have been obvious when a POSITA would have reached the claimed invention through routine experimentation.

104. I understand that one may establish obviousness by combining or modifying the disclosures of the prior art to achieve the claimed invention. It is also my understanding that where there is a reason to modify or combine the prior art to achieve the claimed invention, there must also be a reasonable expectation of success in so doing to render the claimed invention obvious. I understand that the reason to combine prior art references can come from a variety of sources, not just the prior art itself or the specific problem the patentee was trying to solve, but that it cannot come from hindsight recognition of the benefits or advantages of the combination. I also understand that the references themselves need not provide a specific hint or suggestion of the alteration needed to arrive at the claimed invention; the analysis may include recourse to logic, judgment, and common sense available to a POSITA.

105. I understand that when there is some recognized reason to solve a problem, and there are a finite number of identified, predictable solutions, a POSITA has good reason to pursue the known options within his or her technical grasp. If such an approach leads to the anticipated success, it is likely not the product of innovation, but rather of ordinary skill and common sense. In such a circumstance, when a patent simply arranges old elements with each performing the same function it had been known to perform and yields no more than one would expect from such an arrangement, the combination would have been obvious.

106. I understand that when considering the obviousness of an invention, one should also consider whether there are any objective indicia that support the non-obviousness of the invention. I further understand that objective indicia of non-obviousness include failure of others, copying, unexpected results, information that “teaches away” from the claimed subject matter, perception in the industry, commercial success, and long-felt but unmet need. I also understand that in order for objective indicia of non-obviousness to be applicable, the indicia must have some sort of nexus to the subject matter in the claim that was not known in the art. I understand that this nexus includes a factual connection between the patentable subject matter of the claim and the objective indicia alleged.

107. Finally, I understand that the U.S. Patent Office (“USPTO”) may rely upon certain exemplary rationales in reviewing patent applications or patents to understand whether the subject matter of the claims would have been obvious. I understand that the following is the list of exemplary rationales relied upon by the USPTO:

- 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 similar devices (methods, or products) in the same way;
- D. Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- E. “Obvious to try” – Choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- F. Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design

incentives or other market forces if the variations are predictable to one of ordinary skill in the art; and

G. 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.

X. COMPARING THE '292 PATENT CLAIMS WITH THE PRIOR ART

A. “A system for providing services to a secure facility, the system comprising:” (Claim 1, preamble); “A system for providing services to a secure facility, the system comprising:” (Claim 24, preamble)

108. Hogg, Shapiro and Rudolf all expressly disclose systems for providing services to correctional facilities (one example of the “secure facilities” contemplated by the '292 patent). While Anderson does not expressly disclose use within prisons or correctional facilities, Anderson expressly discusses use in secure environments and facilities such as military facilities: “computer users can view data on a computer-controlled display *in a variety of secure and unsecured environments* with greater security from unwanted and undetected eavesdropping and tampering”, such as found “commonly in *government, scientific, engineering, and military applications....*” *Id.*, 4:28-37, 9:20-38. Military facilities, correctional facilities, and law enforcement facilities all share similar risk profiles from a technology perspective. Each contains confidential records and is a location where secure transactions are performed. That security applies to both physical and digital records. For example, a military facility may be used for planning tactical operations or maintaining the certifications and qualifications of military personnel. Similarly, a correctional facility may be used to create and maintain prisoner transfer and transportation plans or to maintain private offender crime, sentencing, and rehabilitation records. Law enforcement facilities host

investigation, arrest, and detainment information. In each of these environments, the chain of custody of records must be maintained and the sanctity of information must be ensured. Similar to prisons, military facilities by their nature require additional levels of monitoring and oversight that are not generally required for the general population.

109. Further, as discussed above, the ‘292 Patent does not limit the meaning of secure facilities to prisons, correctional facilities, and the like. The ‘292 Patent states that its systems could be used in “any facility requiring consolidated secure services.” Ex. 1001, 2:43-45. Anderson certainly provides consolidated secure services. For example, Anderson states, “[t]hese capabilities are, in some exemplary embodiments, implemented in such a way as to **support centralized security policies and enforcement of these**, with audit data maintained to permit later analysis of adherence to them.” Ex. 1007, 7:64-8:1. Centralized secure services are analogous to consolidated secure services. In the patents, “centralized security policies” and “consolidated secure services” are used to express the organizations’ planned and designed security policies in technical platforms and operational environments that protect the actions and data of the organization.

110. Further, regardless of whether “secure facility” is narrowly construed to be limited to prisons and the like, a POSITA would still have found it obvious to use the system disclosed in Anderson in such as setting as disclosed in Hogg, Shapiro and Rudolf. For example, Anderson states that “[s]ome means of permitting display of information to authorized users, while detecting, limiting or preventing disclosure to others, is needed.” Ex. 1007, 2:4-6. This exemplary goal of Anderson is very similar to an exemplary goal of Hogg, which is expressly directed for use in prisons: “a desire exists for monitoring calls for detecting and/or preventing unauthorized activity during the calls, such as detecting a call to an unauthorized party...” Ex. 1006, 3:47-50. Consequently, because both Anderson

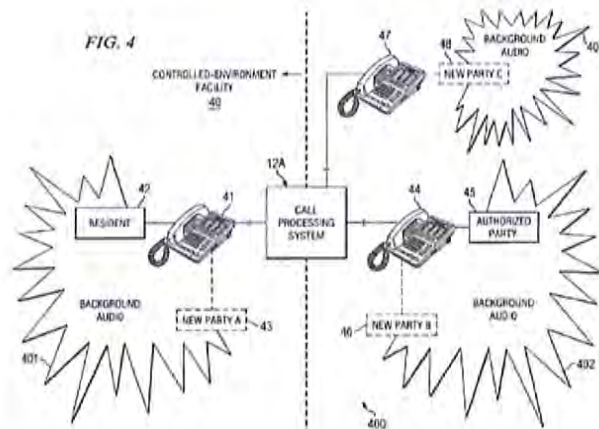
and Hogg are concerned with limiting information to authorized parties, a POSITA would have considered it obvious to consider Anderson's technology for use in the prison environments of Hogg.

- B. “a kiosk located at a secure facility, the kiosk comprising a processor, display, speaker, microphone, and a camera; and”** (Claim 1.a); **“A kiosk for providing facility services in a secure manner, comprising: a computer processor; a memory connected to the processor via a bus; a camera connected to the bus for inputting video communications; a microphone connected to the bus for inputting audio communications; a speaker connected to the bus; a touchscreen display connected to the bus; and a network interface connected to the bus for communicating with a server via a network connection,”** (Claim 15P; Claim 15.a-.g); **“a method for monitoring use of an interactive kiosk during a video transmission, comprising:”** (Claim 22, preamble); **“a plurality of kiosks located at a secure facility, each kiosk comprising a processor, display, speaker, and microphone; and”** (Claim 24.a)

111. As discussed above, the '292 Patent broadly defines kiosks beyond the ordinary definition of a kiosk to include not only traditional kiosks, but to include *“a standalone structure, a personal computer, a laptop, a mobile device, or a tablet computer device.”* Ex. 1001, 8:47-50. As such, Hogg, Anderson, Shapiro and Rudolf all disclose kiosks located at secure facilities.

112. Hogg discloses kiosks (*e.g.*, PDA or laptop) having audio/video capabilities located at the correctional facility. “Embodiments of the present invention can be applied for monitoring various types of calls. ...*For instance, a video communication is a call.... Additionally, if a video communication further comprises an audio portion....* As another example, a handwritten communication, such as a handwritten message input to a computer device, such as a personal digital assistant (PDA) or laptop computer, and communicated via a communication network....” Ex. 1006, 5:29-54.

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292



Ex. 1006, Fig. 4.

114. Anderson also discloses kiosks (*e.g.*, personal computers, laptops, mobile devices, tablet computers). Each kiosk includes a processor, display, speaker, microphone and a camera. “The exemplary system (1000) includes a computer (1050).... Computer 1050 is electronically coupled with a display device (1200) including a *viewing surface or display* (1250) that is viewed by a user (1300) whose ability to view intelligibly content displayed on the display at a gaze point “g”, as determined in part using an *image sensor (1400), such as a camera (e.g., a “webcam”)* ... electronically coupled with a security processor (not shown).... *Each of these elements is of standard design and construction....*” Ex. 1007, 8:44-62. *See also, id.*, 8:63-9:19.

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

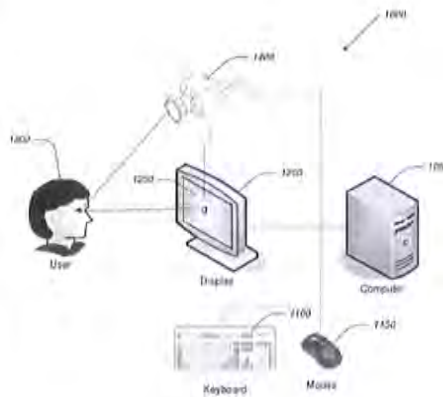


FIGURE 1

Ex. 1007, Fig. 1.

115. Anderson continues, "...the device's *speakers* or *microphone* (or both) are muted when privacy mode is activated." *Id.*, 16:13-16. This shows that the Anderson kiosks include speakers and microphones, which is expected in such types of computing devices.

116. Anderson continues, "FIG. 9 shows a schematic drawing of ... a plurality of devices of various types, such as a *tablet-based portable computer* (9030), a *PDA* (9050), a *desktop computer* (9070), and a *laptop or netbook computer* (9090). The users being recognized (9020, 9040, 9060, and 9080) can be different users...." *Id.*, 21:52-61.

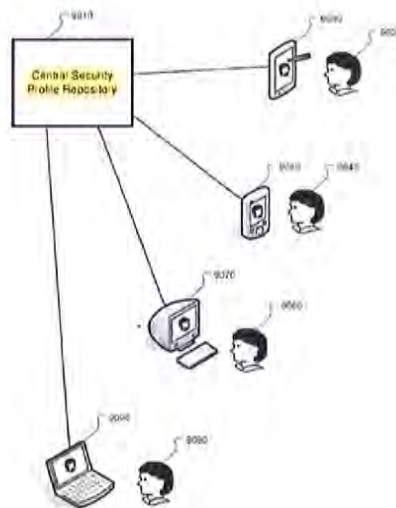


FIGURE 9

Ex. 1007, Fig. 9.

117. Anderson continues, “FIG. 14 depicts ... where a *video capture device* (14010) sends video data (14020) to a video device monitor (14110) component in a computing device (14120). The video device monitor passes video data (14130) to applications (14140) ... while also requesting the display *processor* (14170) to provide an on-display indication of the video capture device's activation status (14160).” *Id.*, 25:65-26:5. “Similar methods can be used to direct, restrict, monitor or indicate the in-use status of other devices (or some combination thereof), such as *microphones*” or *speakers*.” *Id.*, 26:14-23.

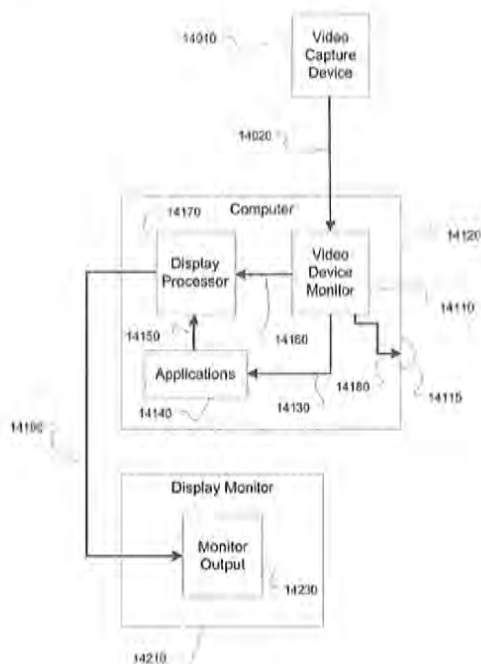


FIGURE 14

Ex. 1007, Fig. 14.

118. Shapiro also discloses kiosks located at the correctional facility. Disclosed kiosk 210, for example, includes a processor 220, a display 191, a speaker 197 and a microphone. *“Another aspect of the invention involves providing a computer-operated kiosk that may be used by individuals (e.g., inmates) in a restrained environment/restricted-access location (e.g., a prison) to browse through a catalog of available digital media or content, such as music....”* Ex. 1008, Abstract. *“The computing device 210 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 180. The remote computer 180 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computing device 210.... In one embodiment of the present invention this computer*

180 may be used to implement a kiosk for delivering digital media to an inmate or as a terminal for displaying correspondence to an inmate.” *Id.*, [0031].

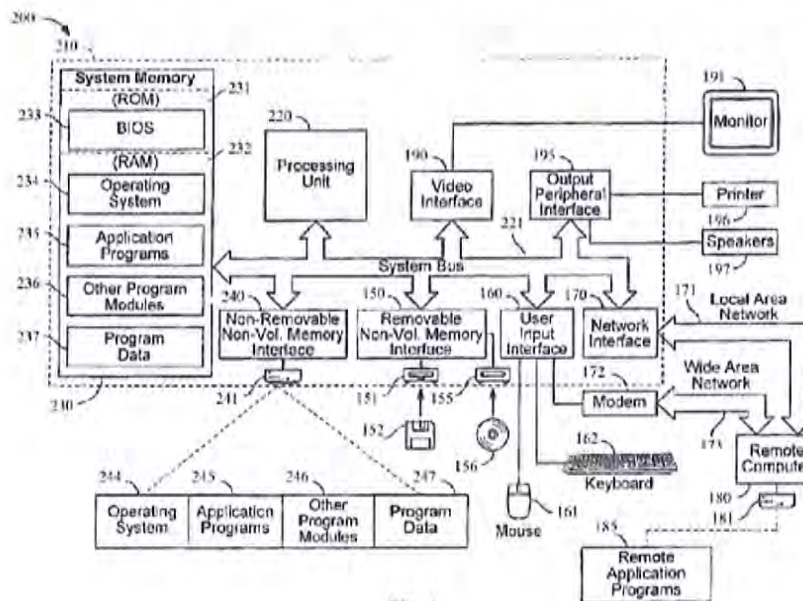


Fig. 1

Ex. 1008, Fig. 1.

119. Rudolf discloses video visitation kiosks (communication stations) located at a secure facility. Rudolf discloses the kiosks include a processor, display, speaker, microphone, and a camera. “The present invention is directed to a video visitation communication system. The system includes a plurality of communication stations, each station having a microphone configured to generate an audio signal, a video camera configured to receive the audio signal and generate a combined audio/video signal for transmission, and a display configured to display a received video signal.” Ex. 1009, [0007]. “Referring now to FIG. 2,” ... “[c]ommunication station 200 includes a station processor 202, a memory 204, and an audio mixer 206. Input and output for communication station 200 may be implemented using an IP camera 212, a handset 214 and a display monitor 216.” *Id.*, [0026]. See also, *id.*, [0030]-[0031].

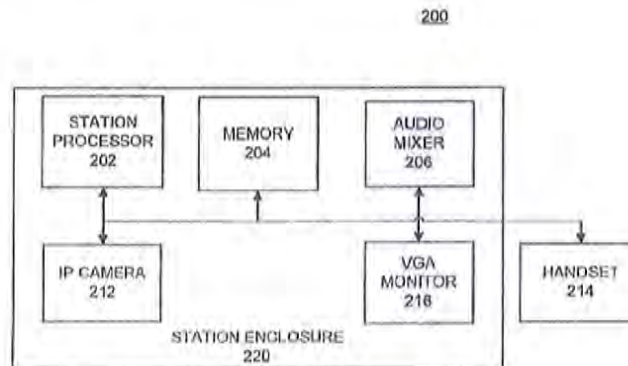


Fig. 2

Ex. 1009, Fig. 2.

120. To the extent not completely disclosed by Hogg, it was well known (or at least would have been obvious) to a POSITA that: PDAs or laptops disclosed by Hogg; personal computers, laptops, mobile devices, tablet computers disclosed by Anderson; and kiosks disclosed by Shapiro would have included a processor, display, speaker, microphone, and a camera as taught by Rudolf, for example. Each device performs the function of allowing the end user to interact with the applications and services provided by the presented applications. Whether input is collected on a PDA's touch screen or laptop's keyboard discussed in Hogg, or a tablet discussed in Anderson, or by the touch screens of the Rudolf and Shapiro kiosks, the intent is to collect information, direction, or responses for processing, then to present the system response on the included display screen, speaker, or other output device. The same would be true for cameras or any other input or output devices connected to the system.

121. To the extent these references do not expressly disclose that the kiosk includes memory connected to a processor via a bus, it was well known and would have been obvious to POSITAs that personal computers, laptops and such have memory connected to the processor via a bus. For example, Shapiro discloses the

kiosk (which, as disclosed above in ¶118, may have the components of computer 210) includes a memory connected to the processor via a bus. “With reference to FIG. 1, an exemplary system that may be used for implementing the invention includes a computing device 210 which may be used for implementing a server. Components of computing device 210 may include, but are not limited to, a *processing unit 220*, a *system memory 230*, and a *system bus 221* that couples various system components including the system memory to the processing unit 220.” Ex. 1008, [0026].

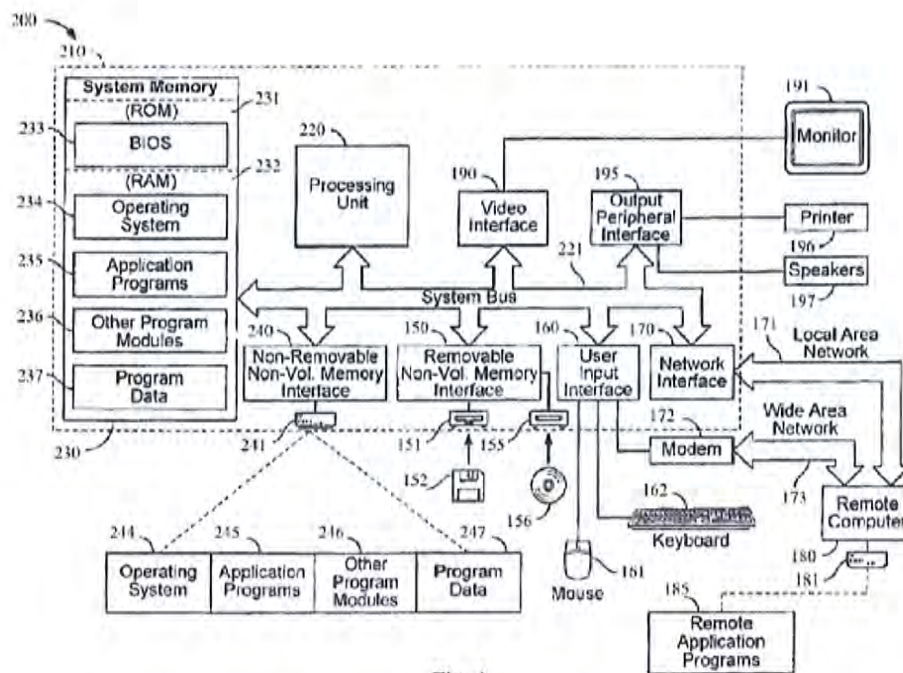


Fig. 1

Ex. 1008, Fig. 1.

122. To the extent that these references do not expressly disclose a camera connected to the bus for inputting video communication, it was well known and would have been obvious to POSITAs that personal computers, laptops and such have cameras connected to a processor via a bus. It would have been obvious for a

POSITA to connect the camera to the system bus 221 of Shapiro as another “system component” as discussed in ¶121 or another “input device” as discussed below in ¶123 for communicating with the processor 220. While not all computers, laptops or tablets include a camera, it would have been obvious to a POSITA that any device used for video calling, video conferencing, or video visitation must be connected to a camera, whether the camera is included as a component within the computer or device, or added via an interface like a USB cable, ethernet cable, Bluetooth, or other mechanism. No matter the mechanism of connecting the device, the video content is captured and sent to the processor via a mechanism as described as a bus. Information Technology staff working in prisons regularly assemble individual components including keyboards, cameras, mice, monitors, speakers, projectors, and various other devices as needed for any specific functionality required for offender management, health care operations, education, or job performance.

123. To the extent that these references do not expressly disclose a microphone connected to the bus for inputting audio communication, it was well known and would have been obvious to POSITAs that personal computers, laptops and such have cameras connected to a processor via a bus. For example, Shapiro also discloses the microphone is an input device connected to the processor via the system bus. “A user may enter commands and information into the computer 20 through *input devices* such as a keyboard 162 and pointing device 161, commonly referred to as a mouse, trackball or touch pad. *Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 220 through a user input interface 160 that is coupled to the system bus*, but may be connected by other interface and bus structures, such as a parallel port, game port or a universal serial bus (USB).” Ex. 1008, [0030]. It would have been obvious to a POSITA that

the camera and microphone of Hogg and Anderson would also be connected to its processor via a system bus as taught by Shapiro.

124. To the extent that these references do not expressly disclose a speaker connected to the bus, it was well known and would have been obvious to POSITAs that personal computers, laptops and such have speakers connected to a processor via a bus. For example, Shapiro also discloses speakers connected to the bus through an output peripheral interface 195. “In addition to the monitor, computers may also include other peripheral output devices such as *speakers* 197 and printer 196, *which may be connected through an output peripheral interface 195.*” Ex. 1008, [0030]. It would have been obvious that the speaker of the disclosed kiosks (of Hogg, Anderson, etc.) would also be connected to its processor via a system bus as taught by Shapiro.

125. To the extent that these references do not expressly disclose a touchscreen display connected to the bus, it was well known and would have been obvious to POSITAs that personal computers, laptops and such have touchscreen displays connected to a processor via a bus. For example, Anderson discloses the kiosk may include a touch screen display. “In one embodiment, one assumption is that a user will be looking at a pointing device cursor, such as a mouse pointer, a stylus, *a touch screen tap location*, or other input device or method, while the pointing device is in use.” Ex. 1007, 14:30-34. Further, it is well known that such computer peripherals are connected to processors via a system bus. For example, while Shapiro does not disclose a touchscreen display connected to the bus; Shapiro discloses a touch pad input device and also discloses a computer monitor – both coupled to the system bus. “A user may enter commands and information into the computer 20 through input devices such as a keyboard 162 and pointing device 161, commonly referred to as a mouse, trackball or *touch pad*. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner,

or the like. *These and other input devices are often connected to the processing unit 220 through a user input interface 160 that is coupled to the system bus...*”

Ex. 1008, [0030]. *“A monitor 191 or other type of display device may also be connected to the system bus 221 via an interface, such as a video interface 190.”* *Id.*

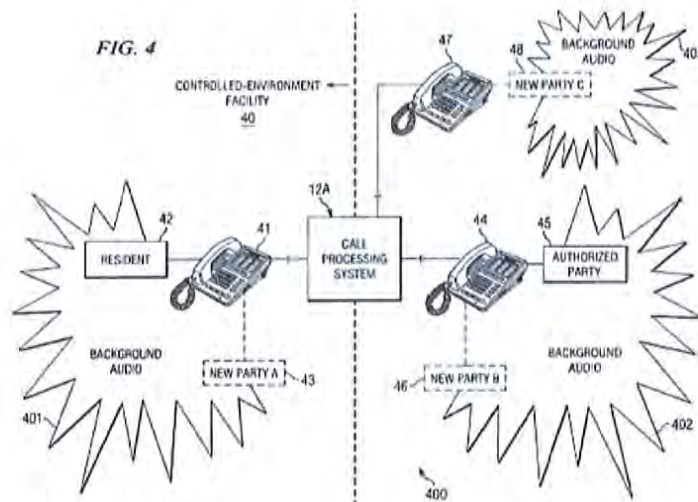
It would have been obvious for a POSITA to combine each of these functions into a touchscreen display of any of the disclosed kiosks according by Anderson and Shapiro.

126. To the extent that these references do not expressly disclose a network interface connected to the bus for communicating with a server via a network connection, it was well known and would have been obvious to POSITAs that personal computers, laptops and such for video conferencing applications have network interfaces, such as Wi-Fi circuitry, connected to a processor via a bus. As discussed below in Section X(C), Hogg, Anderson, Swanson, Shapiro, etc. disclose that the kiosks may be connected to servers via a network connection, which would necessitate or render obvious the user of a network interface connected to the system bus. For example, Shapiro discloses that the kiosk includes a network interface (network interface 170 or modem 172) connected to the bus (see Fig. 1) for communicating with a server via a network connection. “When used in a LAN networking environment, the computing device 210 is connected to the LAN 171 *through a network interface or adapter 170.*” Ex. 1008, [0032]. Within a prison, jail, or other secure facility, IT staff configure computers to fulfill the requirements of the specific need, in the specific environment. At times, a stand-alone computer is used to ensure there is no communication between offenders or other parties. An example would be a computer in a law library. In that instance, a computer with a monitor, processing unit, keyboard, and large hard drive or optical drive is used by an offender for research of case law. That use and environment has no need of connectivity or connection to other computers or functionality. In other instances, a

classroom for example, computers would need to be connected to a network to allow students to share work and assignments with the instructor, and the solution often allows instructors to observe the in-progress work of students from the instructor's workstation (computer).

- C. **“a server that communicates with the kiosk via a network connection, the server comprising a server processor, a network interface unit, and a computer memory;”** (Claim 1.b); **“a server that communicates with the kiosks and a device of an outside party via one or more network connections, the server comprising a server processor, a network interface unit, and a computer memory”** (Claim 24.b); and every other claim element calling out a server.

127. Hogg discloses that its call processing system 12A is implemented in a central server. “Turning to FIG. 4,” [...] “*call processing system 12A may be implemented in a central server that monitors calls for one or more controlled-environment facilities.*” Ex. 1006, 12:30-42.

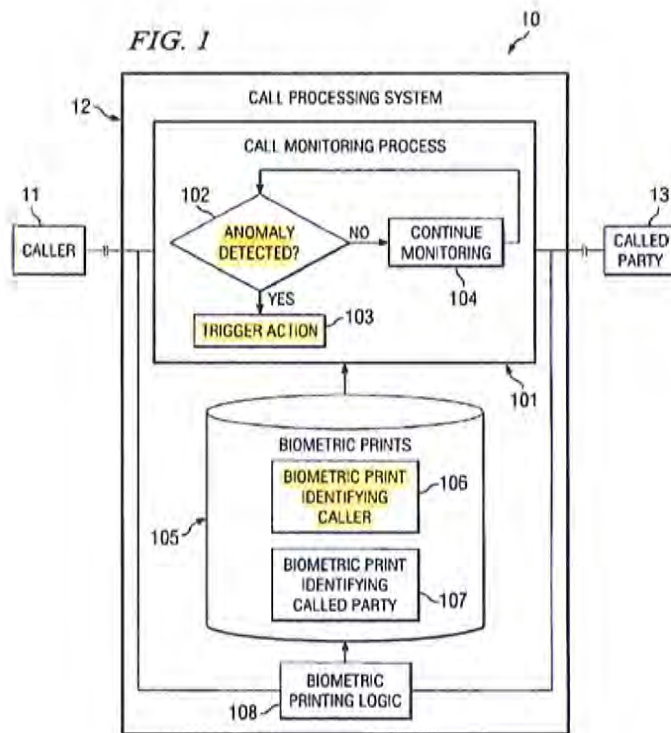


Ex. 1006, Fig. 4.

128. Hogg discloses that the call processing system 12A (which may be implemented in a central server) are executable by a processor. “The exemplary

operational flow of FIG. 3 may, for example, be implemented via software executable by a *processor*. Further, various operational aspects described herein for the call processing system, such as the biometric printing logic and call monitoring process, may be implemented via software executable by a *processor*.” *Id.*, 15:62-67.

129. And Hogg discloses in Fig. 1 (and associated discussion of Fig. 1) that the call processing system 12, situated between a called party 13 and a caller 11, is connected between such parties via a network, such as a wireless network, the Internet or the like. “In exemplary system 10, a caller 11 makes a call to called party 13. *Such a call may be a telephone call, video conference call, or other communication conducted over a communication network, such as a circuit-switched or packet-switched network as examples. Id.*, 9:4-9. For example, the communication between the parties may be communication over any suitable communication network now known or later developed that supports communication between parties, *such ... wireless network, the Internet or other wide-area network (WAN), a local-area network (LAN), or any combination of the foregoing, as examples. A call processing system 12 is provided for monitoring the call. In this example, call processing system 12 comprises biometric printing logic 108 that is operable to generate biometric prints 106....” Id.*, 9:9-19. [S]uch biometric prints may be stored to a *computer-readable data storage medium 105....” Id.*, 9:20-25. As the call processing system 12 is connected to the parties 13 and 11 via a network it would have been expected, inherent and obvious that the connection would be via a network interface unit. Without such network interface unit, no network connection could be made at all.



Ex. 1006, Fig. 1.

130. Anderson also discloses that its security software can be implemented on a server (such as a web server available to all users via a Web browser) communicating with the kiosk via network connection. “In some embodiments, *the methods and software of the invention* are implemented as a browser plugin... In more specific embodiments such as this, *the software can be provided on the web server side, and it would be available to all users (or mostly all depending on browser)...*” Ex. 1007, 17:9-21.

131. Anderson also discloses that its systems can be implemented using a client-server type arrangement. “Those having ordinary skill in the art will understand that the systems illustrated in FIGS. 1 and 2 encompass systems in which the illustrated connections are physical (e.g., by direct cable connection) and logical (i.e., the connections are either remote, such as over a network connection

in a *client-server type arrangement*, or through wireless connections).” *Id.*, 9:20-38.

132. Shapiro also discloses a server that communicates with the kiosk via a network connection; and that the server includes a server processor (processing unit 220), a network interface unit (network interface 170) and a computer memory (System Memory including ROM 231 and RAM 232). “The present invention may be implemented in one or more *servers*, one or more client devices, including computer terminals or portable client devices, or a combination thereof.” Ex. 1008, [0021]. “*An exemplary computing device for implementing a server is illustrated in FIG. 1.* For example, the computing environment illustrated in FIG. 1 may be used to implement a database server, an email server, a DNS server, a POP/IMAP server, a digital fulfillment server, a media server, a local server, a global server, etc.” Ex. 1008, [0022].

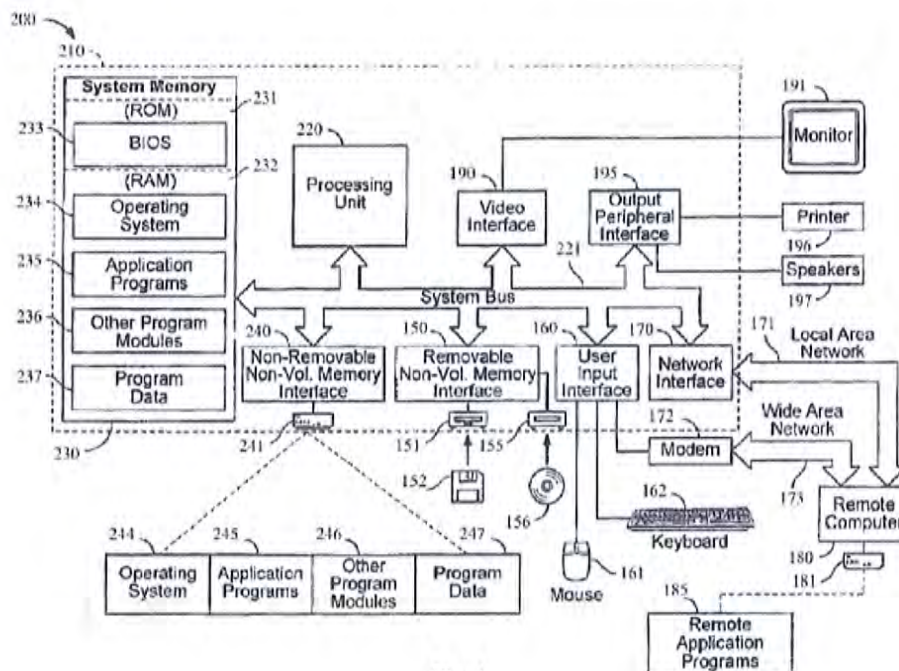


Fig. 1

Ex. 1008, Fig. 1.

133. Fig. 7 of Shapiro is one of many examples of the kiosk communicating with the server via the network connection (i.e., via web services over an internet connection). “FIG. 7 illustrates a method for processing a purchase transaction for a player using the kiosk application. At step 701 the inmate places an order using the kiosk terminal. The order is communicated to the global server via web services.” *Id.*, [0163].

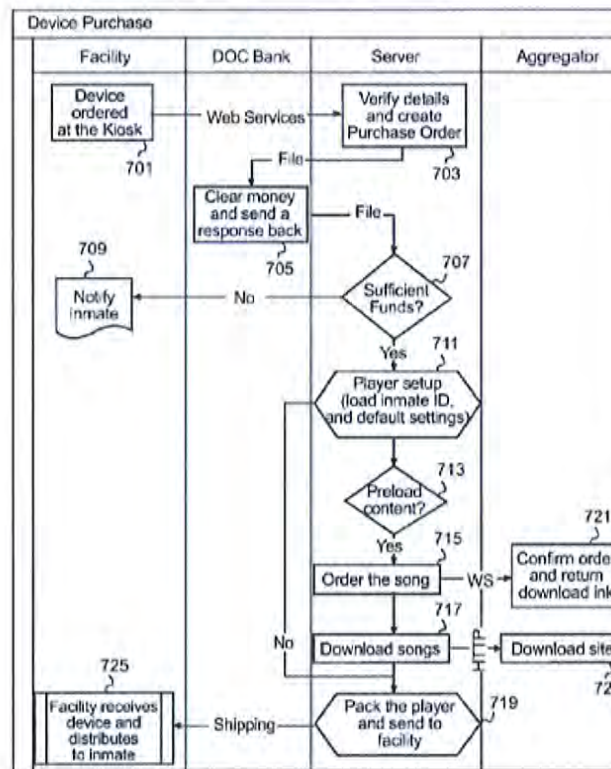


Fig. 7

Ex. 1008, Fig. 7.

134. Swanson discloses kiosks (user computers 34), configured to receive communications from the kiosk camera and microphone and transmit and receive audio and video of the communications to and from the server 112 via the network 110. “Communications between each of Users A-F may be carried out on a two-

way basis from the network 10, with data sent to and received from each of the Users A-F over the communications lines 14.” Ex. 1010, 4:12-16.

“[C]ommunications over the network 10 between Users A-F may be ... streaming.” *Id.*, 4:28-33. “In a streaming video communications sessions application, each User A-F may have one or more cameras ... and/or microphones from each of which is streamed a continuous, real-time data...” *Id.*, 1010, 4:33-40.

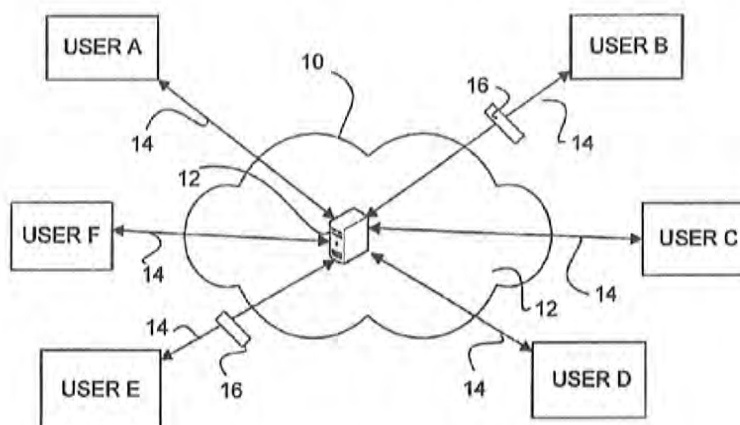


FIG. 1

Ex. 1010, Fig. 1.

135. Swanson continues, “[t]he one or more computers 34 at each of the Users A-F may be used to receive and send all of the video, audio.... Examples include ... media communication devices such as processor enabled phones or personal digital assistants...” *Id.*, 6:61-7:17.

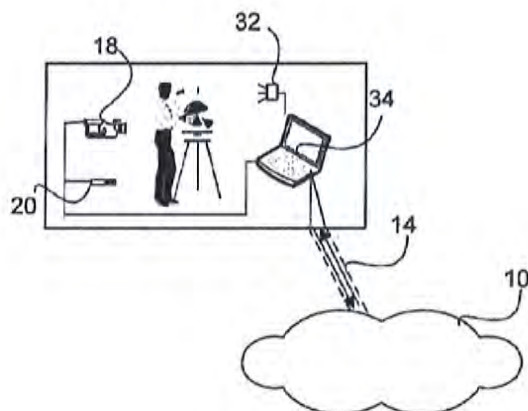


FIG. 3

Ex. 1010, Fig. 3.

136. Swanson continues, “FIG. 4 is a schematic of an example network to carry out a videoconference.... Many aspects of the network are consistent with the network 10 ... with like numbers used in the 100 series for convenience. The network 110 includes one or more conference servers 112 over which any number of users 1-17 can jointly participate in a video conference....” *Id.*, 10:36-11:9.

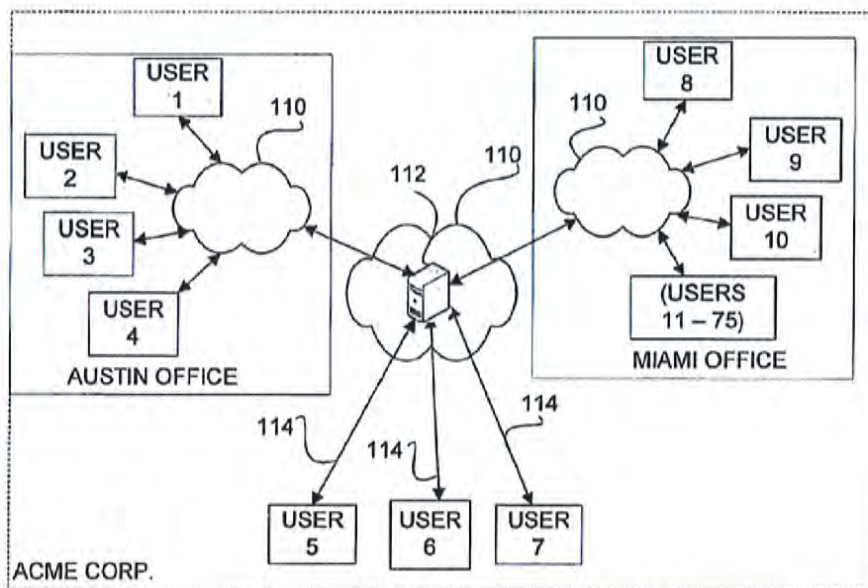


FIG. 4

Ex. 1010, Fig. 4.

137. Rudolf also recognizes that a server computer may be used in a correctional facility to handle video visitations between visitor communication stations (i.e., visitor kiosks) and inmate communication systems (i.e., inmate kiosks). “The correctional facility may install a number of visitor communication stations in a visitor center. The facility may also install a number of inmate communication stations within the facility. A switch matrix connected to a ***communication management server*** may be used to connect any visitor communication station to any inmate communication station.” Ex. 1009, [0003]. The communication management system 130 of Rudoff performs these functionalities and more. For example, see claim 1: “a communication administration station configured to perform steps stored on a computer readable medium to establish a communication channel between the first communication station and the second communication station.” *Id.*, claim 1. As such, it would have been well understood that communication management system 130 could have been or would have been embodied in or on the server computer as disclosed by Rudolf. Because of the nature of phone calls, video calls, telemedicine interactions, or any other communication between offenders in a secure facility to other parties, it is necessary to manage, record, and oversee the interactions centrally. Use of a centralized solution is needed to effectively manage multiple connections in use by multiple offenders at the same time. The solution, then, would employ software installed on a centralized computing device that is commonly called a “server.” That server acts as the control point for the interactions, allowing staff to monitor the progress and content of communications from a single observation point, rather than trying to physically interact with each communication directly.

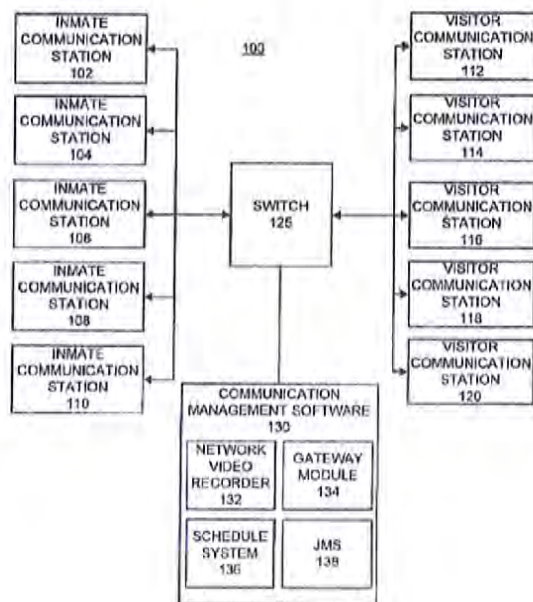


Fig. 1

Ex. 1009, Fig. 1.

138. Rudolf also discloses that the communication administration station 130 may include a network video recorder 132, which receives video streams over a network for recording the video visitations. *Id.*, [0024]. As such, the server on which the communication administration station 130 and network video recorder 132 resides would necessarily have a processor, computer memory and a network interface unit to be able to receive and record such video streams. In a simple consumer example, a Video Cassette Recorder (VCR) can be connected between a television and an antenna or cable connection. This provides the ability to record the flow of images and audio (streams) presented on the TV. In a communication system (network) of devices in a correctional facility, the end user devices (kiosks, tablets, etc.) would be used for both sending (camera) devices and receiving (monitor/speaker) devices. To enable the communication, each device requires memory to store and hold the information, a processor to configure and package

the information into transmittable data packets, and a network interface used to connect the device to a transportation network.

139. As such, a POSITA would understand that any of the software/computer functionality (opposed from functionality that is necessarily performed by the kiosk) of Hogg, Anderson, Shapiro, Rudolf and so forth could be performed on a server, such as the server side of a client-server arrangement. Locating software functionality on a server is routine. From the inception of computers, servers have been used to house the processing and storage that is shared with other devices. This concept originally took the form of a mainframe computer connected to remote terminals. Those terminals performed simple functions like the ability to present data on a screen and collect input via a keyboard. Other input and output devices were possible, including sensors and printers. As computing technology matured, personal computers, tablets, and other devices have added capabilities that did not previously exist. While those devices now have some functionality that can be accessed in "stand-alone" mode, without a connection to a server, they are most often utilized in a "connected" mode, using a network to connect to a server that provides services requested by the user of the device. Those services could be anything from retrieving email from a mail server, to data from a database server, or connecting a calling party to a called party in a communication system.

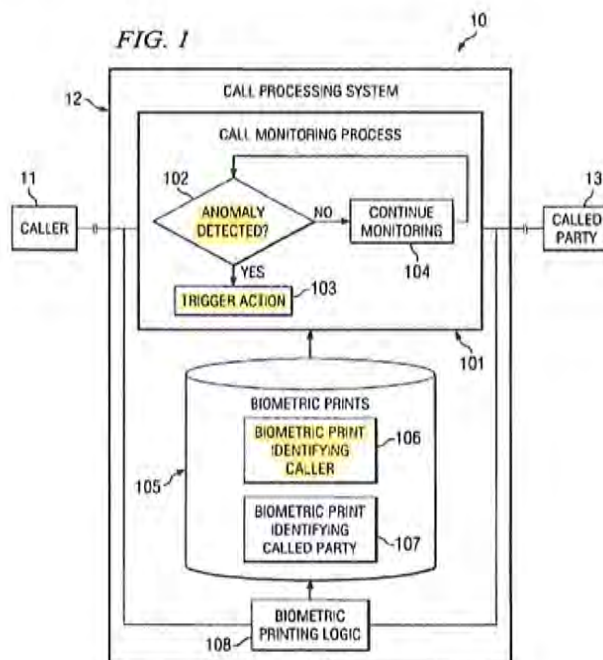
140. While Hogg does not expressly disclose the server includes a network interface, it would have been obvious and expected that the server of Hogg (implementing call processing system 12) would include a network interface to implement such a network connections between the caller 11 and called party 13. It is well known and would have been obvious that such servers in the disclosed client-server arrangement would include a server processor, a network interface unit and a computer memory as disclosed, for example, by Shapiro. While it is

possible to connect devices directly to each other, known as peer-to-peer networking, there is still a logical server and logical server embodied in each "peer" device. The usual configuration in a correctional institution, though, would be connecting an end user device to a remotely placed physical server, or servers, via a network interface and network.

141. Consequently, to the extent not completely disclosed by Hogg; Shapiro, Anderson and Swanson disclose that it is well known to use a server that communicates with the kiosk via a network connection and that the server includes a server processor, a network interface unit and a computer memory. And it would have been obvious to utilize the network-based kiosk/client-server arrangements disclosed in Shapiro or Swanson, for example as the kiosk-server arrangements referenced in Hogg – rendering predictable results. In general, the devices discussed in Hogg, Shapiro, Anderson, and Swanson all describe components in a client-server network. The client-server model distributes workload among the devices connected via a physical or logical network. In these patents, the kiosks, tablets, PCs act as the "clients", used to capture the inputs (audio, video, and interactions with the device) and transmit them to the "server(s)" that perform the management, processing, storage, or distribution of the data. Any certified IT professional, or POSITA as defined in this report would understand and accept these configurations and anticipate the performance and results of the system.

- D. **“the kiosk being configured to receive communications from the camera and microphone and transmit audio and video of the communications to the server via the network connection”** (Claim 1.c); **“wherein the kiosk ... records audio and video communications and transmits the audio and video communications to the server”** (Claim 15.h); **“using a camera of the kiosk to capture video of a user of the kiosk during use of the kiosk; transmitting the video to a server;”** (Claim 22.a-b)

142. As discussed above, Hogg discloses video calls between a caller 11 kiosk and a called party 13 kiosk, monitored by a call processing system 12, which may be situated on a server. As such, it would have been expected and obvious that both the caller 11 kiosk and the called party 13 kiosk would receive communications from the respective kiosk's camera and microphone and transmit video and audio to the server via the network connection between the kiosk and the server. Even in classic telephone systems, an end user device (telephone) uses a network to connect to a central server that then directs (routes) the call to the appropriate receiving party, that party then using a device (telephone) to receive the call. The server maintains that pathway until the call ends. In a video call or video visit, the scenario is the same. A POSITA would naturally expect a client device (kiosk) to capture the inputs (audio, video, keyboard, etc) and transmit them via a network to a server which then passes the appropriate information (data) to the other client (Kiosk). The server itself may modify, store, augment, or otherwise process the data as necessary for the service that is being utilized.



Ex. 1006, Fig. 1.

143. Anderson also discloses that its kiosk is configured to send receive video communications from the video capture device 10010, such as a webcam, and transmit the audio/video to the user attention processor 10040 containing the security software. “Exemplary embodiments of the current invention can use various sensors, *such as video input devices (e.g., “webcams”)*, to detect and identify specific individuals using techniques such as face recognition.” Ex. 1007, 10:54-57. “FIG. 10 depicts a schematic diagram of an exemplary embodiment wherein a *video capture device (10010) provides video data (10020)* to a computer device's (10030) *user attention processor (10040)*. The user attention processor analyzes the video data to identify face-like objects, perform facial recognition, and ... determines the display portions to obscure, if any, and the proper method of obscuration consistent with current option settings....” *Id.*, 23:16-35. It is well understood that video capture devices and video input devices such as webcams include microphones such that the devices transmit both video and audio data.

Declaration of Russell J. Nichols in support of petition for *inter partes* review of U.S. Patent No. 9,030,292

While the initial versions of personal computers or laptops may not have included cameras and microphones, the advent of video conferencing, multi-media training, and other functionality has made the expectation that an end-user computing device of any sort typically contain a microphone and camera. In the timeline of the '292 Patent, a POSITA would expect any device expected to be used in this environment and functionality to contain both a camera and a microphone to capture both video and audio information.

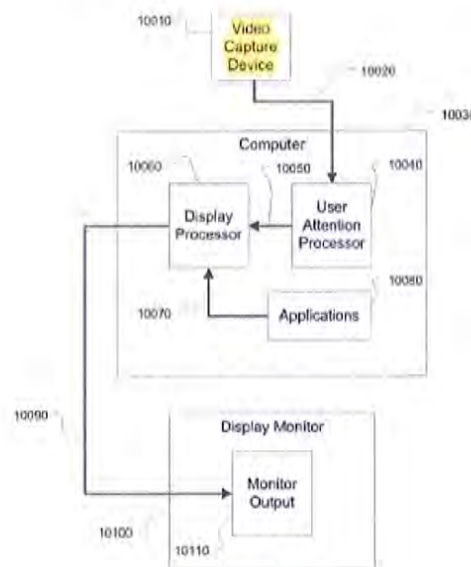


FIGURE 10

Ex. 1007, Fig. 10.

144. As I discuss above in ¶¶130-131, Anderson discloses that the operations of the user attention processor 10040 (as well as many other operations of Anderson) may be implemented on a server. As such, when transmitting the audio/video from the video capture device (i.e., webcam) to the user attention processor, such audio/video would necessarily be (or obviously would have been) be transmitted to the server in that case.

145. As also discussed above in ¶¶134-136, Swanson discloses kiosks (user computers 34), configured to receive communications from the kiosk camera and microphone and transmit and receive audio and video of the communications to and from the server 112 via the network 110.

146. Rudolf also discloses that the kiosks are configured to transmit the audio and video to the administration station 130 over a network when the communications are intended for the second kiosk located in the visitation area for the purpose of allowing the server to record the visitation. “According to an alternative embodiment, communication *administration station 130 may include a network video recorder (NVR) 132*. A network video recorder is a digital recording system that *receives digital images/video streams over a network* and records them on a hard disk in a digital format. ... Advantageously, *NVR 132 may be coupled to switch 125 and configured to receive audio/video signals from both the inmate communication station and the visitor communication station, such that NVR 132 can create a complete video record of the visitation.*” Ex. 1009, [0021]. As discussed above, it would have been obvious and expected that Rudolf’s administration station 130 could or should be implemented on a server as disclosed by Anderson and Shapiro for example. In any secure facility, a POSITA would naturally expect a centralized device (server) to be configured to capture a complete communication. While the functionality of recording the communication could be accomplished at each “client” (kiosk, tablet, computer), staff would then need to combine separate recordings to form a single, unified view of the entire exchange of information. Consequently, a natural expectation would include a server with the capability to capture the entire flow of conversation, from any of the participants, in the natural flow and order of the conversation, even if the parties are speaking (providing audio), moving (providing video) or otherwise interacting with the communication system.

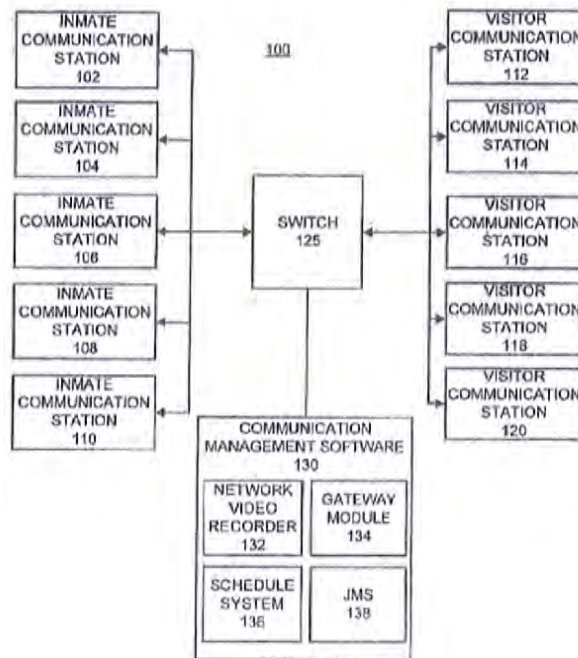


Fig. 1

Ex. 1009, Fig. 1.

147. Rudolf also discloses that the server (administration system 130) gateway module 134 also “enables traditional video conferencing” between the communication stations in the visitation areas and those at the public defenders’ office. “According to yet another exemplary embodiment, administration station 130 may include a gateway module 134. *Gateway module 134 is configured to enable traditional video conferencing between a system 100 communication station and an external videoconferencing system, such as in a public defenders office, a court arraignment hearing, etc.* Gateway 134 may include video conferencing security software such as signal encryption, gateway services, etc.” *Id.*, [0022]. It is well known and would have been obvious that such “traditional video conferencing” would require the kiosks to send captured audio/video to the video conferencing server over a network. This functionality greatly simplifies the

process of pre-trial information collection and is even used for virtual arraignments and testimony. By allowing this functionality, the risk of transporting offenders or the cost of staff traveling to secure facilities is greatly reduced.

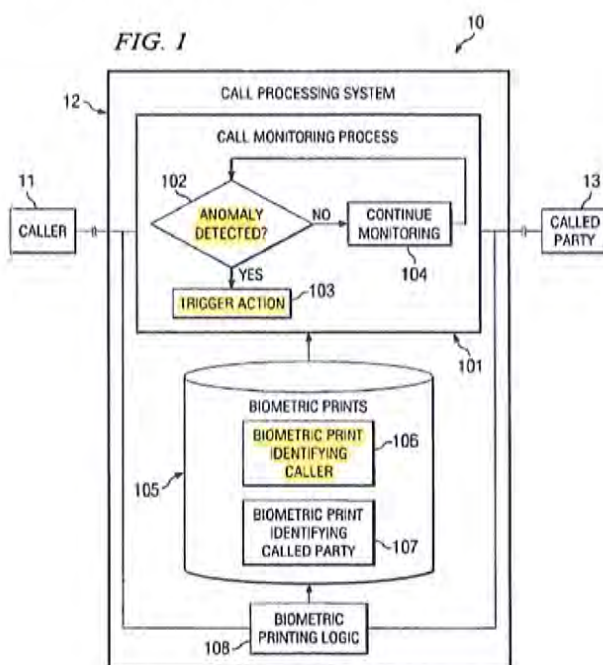
148. Anderson and Swanson show it would have been obvious in Hogg that its kiosk is configured to receive audio/video communications from its video capture devices and transmit the audio/video to the user call processing system 12 on a server via a network connection. It would have been obvious and predictable based on the combined disclosure of Hogg, Anderson and Swanson, therefore, that Hogg call processing system 12 of Hogg when implemented on a server would be configured to receive communications from the camera and microphone and transmit audio and video of the communications to the server via the network connection. While the specific terminology used in each of the prior art patents differ, the technology platforms contain the same functionality. Clients (kiosks, computers etc.) are used to collect the input (video, audio, interactions with the devices) which is transmitted via a network interface and network infrastructure (physical or wireless) to a server which processes, saves, or amalgamates information and then may transmit the information to other devices, including kiosks, servers, tablets, computers, etc. on the network.

E. “wherein the server records the audio and video and transmits the audio and video to a destination;” (Claim 1.d)

149. Hogg discloses its call processing system 12 (which may be on a server as discussed above) recording a video call if the call processing system detects an anomaly in a video call. “Call processing system 12 further comprises a call monitoring process 101 that, as discussed further herein, *is operable to monitor communication between caller 11 and called party 13, and based at least in part on the biometric prints detect anomalies occurring in the call, such as a change in the parties participating in the call. ... If determined that an anomaly is detected,*

such as a change in the parties participating in the call, then a responsive action may be triggered in block 103, such as notifying appropriate personnel, **recording the communication** (e.g., for future investigative purposes), and/or terminating the call, as examples. While no anomaly is detected, operation advances to block 104 to continue monitoring of the communications between caller 11 and called party 13.” Ex. 1006, 9:26-44.

150. Further, as discussed above in ¶127-129, Hogg discloses video calls between a caller 11 kiosk and a called party 13 kiosk, monitored by a call processing system 12, which may be situated on a server. As such, it would have been expected and obvious that the server situated between the caller 11 and the called party 13 would also transmit audio and video of the video call to the destination kiosk of called party 13. As explained above, both the caller 11 kiosk and the called party 13 kiosk would receive communications from the kiosk’s camera and microphone and transmit video and audio to the server via the network connection between the kiosk and the server.



Ex. 1006, Fig. 1.

151. To the extent not completely disclosed by Hogg, Rudolf discloses that the server (administration station 130) may be configured to record audio and video; and discloses that the server (administration station 130) may transmit the video conference audio/video from a prisoner's communication station to/from a visitor's communication station. "According to an alternative embodiment, communication *administration station 130 may include a network video recorder (NVR) 132. A network video recorder is a digital recording system that receives digital images/video streams over a network and records them on a hard disk in a digital format.* Viewing and management of the NVR generally takes place remotely over the network via the administration station 130. Advantageously, *NVR 132 may be coupled to switch 125 and configured to receive audio/video signals from both the inmate communication station and the visitor communication station, such that NVR 132 can create a complete video record of the visitation.*" Ex. 1009, [0021].

152. Anderson also discloses the server recording the video/audio data and transmitting it to a destination, such as to others in a video conference. "***In some embodiments the video data is actually recorded.***" Ex. 1007, 19:32-33. "Alternatively or additionally, some exemplary embodiments alert the current user to the presence of such unauthorized display viewers, ***record the video input device data feed for later analysis, ...***" *Id.*, 19:47-50.

153. It would have been obvious based on the combined disclosure of Hogg, Anderson, Rudolf and Swanson, therefore, that Hogg's call processing system when implemented on a server would be configured to record the audio/video of the video call and transmit it to the destination on the other end of the video call "to create a complete video record of the visitation" as taught by Rudolf or record

the video “for later analysis” as taught by Anderson. This capability is expected in a secure facility and has been in existence for standard voice telephone calls for many years. The ability to store, replay, and analyze phone and video communications is paramount for staff in investigations and offender management to ensure continued safety in the secure facility.

- F. **“wherein the kiosk is configured to authenticate the identity of a user of the kiosk by verifying log in information entered by the user and also performing a biometric verification;”** (Claim 1.e); **“wherein the kiosk authenticates a user by receiving personal log in information and comparing the received personal log in information against a known personal log in information associated with the user, verifies the user's identity using a biometric verification,”** (Claim 15.h)

154. Hogg discloses that *both* parties to a disclosed video call are pre-authorized, “... face prints are obtained for parties that are *authorized to participate in the call...*” Ex. 1006, 4:4:55-62. Hogg discloses that its call processing system 12A is configured to authenticate the identity of a kiosk user, such as called party 45. “In the exemplary system 400, resident 42 of controlled-environment facility 40 uses telephone 41 to call an authorized party 45. Authorized party 45 can accept the call and audibly communicate with resident 42 via telephone 44. *Call processing system 12A may use various techniques for determining that the called party 45 is authorized to participate in the call.*” *Id.*, 12:43-49.

155. Hogg also discloses that a form of user authentication for both parties on a call involves a combination of biometric verification (e.g., voice print) and login information entered by the user (e.g., PIN#), “... *a voice print may have been generated for caller 11 and called party 13 during a previous call, and such voice print may be stored to a computer-readable storage medium and associated with the respective party with which it identifies ... a voice print previously generated*

for caller 11 may be associated with a personal identification number (PIN) that the caller is required to input when initiating a call. Thus, call processing system may receive the PIN and look-up the previously generated voice print for the caller.” Id., 10:56-65.

156. Anderson discloses that the kiosk (which includes a webcam as discussed above and a log-in display 3140 as disclosed below) authenticates the identity of a user by log in information (e.g., passwords) and by biometric verification (e.g., facial recognition). “FIGS. 3A-3C illustrate certain aspects related to *user authentication* ... FIG. 3A illustrates the appearance of a user's face ... *by a webcam* ... FIG. 3B illustrates the provision of a user identification and authorization dialog ...” Ex. 1007, 6:49-51. “FIGS. 3A-3C are diagrams representing an *exemplary authentication* ... Referring to FIG. 3A, *the video input (3010) provided by a video input device or image sensor (not shown), comprises a face-like object (3020). In some exemplary embodiments, the face-like object is analyzed and compared to the faces of known individuals in order to perform facial recognition and identify the individual in front of the video input device. ... [T]he exemplary embodiment in this example is using the facial recognition as a primary means of authentication for convenience. The user must still enter a password into the password field of the login display (3140, FIG. 3B) to confirm his identity and be granted access as the current user.” Id., 11:28-51.*

“Referring ... to FIG. 3A ... gestures can be used as a form of *authentication*, whether instead of, or in addition to, more traditional forms of *multi-factor authentication, such as passwords, token keys, biometric data, or smartcards.*” *Id.*, 11:52-56.

157. Shapiro also discloses that each inmate needs to log into the kiosk using a unique ID so that the kiosk will authenticate the user. “*Inmates log into the kiosk and then browse through the catalog of specific offerings.*” Ex. 1008, [0172]. “In

addition to facilitating the downloading of content into the player, *the kiosk application is responsible for the Player maintenance and control in accordance with one embodiment of the invention. Each Player is registered to one inmate and includes a unique ID to be matched with a specific inmate ID.* Each kiosk can only access the inmate's account on the Local Server 1912.” *Id.*, [0199]

158. To the extent that Hogg does not disclose that the kiosk authenticates the user using a combination of biometric information and log-in information, it would have been obvious for Hogg to have its kiosks perform such authentication as taught by Anderson as Anderson shows that such multi-factor authentication performed by the kiosk was customary and predictable for users in secure environments. Combining multiple methods of authenticating a person is considered Multi Factor Authentication (MFA). It usually involves at least two items from: 1. something you have (a token, ID,); 2. something you know (password / PIN); and 3. something you are (biometric capture). As an example in the general public, consumers are now used to MFA in banking situations by providing a login credential (username and password) and a server-generated PIN that is communicated to the user at the time of login. The same intent is used in a secured facility and has been in use since long before the time of the 292 Patent. Usually, an offender making a phone call is identified by institution staff using a physical ID card or other facility record and a visual inspection of the offender, then the offender could use a login credential (PIN, account number).

- G. **“wherein, after the user identity has been authenticated by the kiosk and during the transmission of the video, the server is configured to periodically extract a frame of the video and perform a check to determine if a face is present in the frame,”** (Claim 1.f); **“wherein, after the user has been authenticated and during a transmission of a video, the video being transmitted from the kiosk to the calling party, the server is configured to periodically extract a frame of the video; and perform a check to determine if a face is present in the frame,”** (Claim 24.f); **“wherein, after the user has been authenticated and during the transmission of the video, the kiosk is configured to periodically extract a frame of the video and perform a check to determine if a face is present in the frame,”** (Claim 15.i); **“periodically extracting, at the server, a frame of the video; performing a check after the user identity has been authenticated by the kiosk and during the transmission of the video, at the server, to determine if a face is present during the frame;”** (Claim 22. d-e)

159. Hogg discloses that call processing system 12 (which may reside on a server as discussed above) monitors biometric information (e.g. facial recognition) of pre-authenticated users/callers, during the video call to check if the expected (e.g., authorized) face is present in the print/frame. “Call processing system 12 further comprises a call monitoring process 101 that, as discussed further herein, is operable to monitor communication between caller 11 and called party 13, and based at least in part on the *biometric prints detect anomalies occurring in the call, such as a change in the parties participating in the call*. Thus, as shown in the example of FIG. 1, call monitoring process 101 may monitor communications between caller 11 and called party 13 and determine in operational block 102, *based on a comparison between the biometric prints 106, 107 and biometric data determined from the communications, whether an anomaly is detected for the call.*” Ex. 1006, 9:26-38. Hogg continues, “..., *in an embodiment in which the communication between caller 11 and called party 13 comprises video of the parties (e.g., via video conference call), then biometric printing logic 108 may*

generate video-based biometric prints, such as face prints, iris prints, etc.

Thereafter, the video communications between caller 11 and called party 13 *may be monitored and compared with the generated video-based biometric prints* to, for example, *detect changes in the parties participating on the call.*" *Id.*, 10:6-14. The act of "monitoring" for anomalies "occurring in the call" means that the facial recognition occurs during the video call (i.e., during the transmission of video). At some predetermined interval, the system is configured to take a "picture" of the face of the party using the camera in the end user device. The picture is transmitted to the server, where the monitoring process and biometric logic compares the features and data points in the recently collected image from an image or reference data that is stored in the server. If the comparison confirms the party is the expected party, the call continues. If it is not, the system takes a remedial action which could include repeating the process for confirmation, pausing the conversation, terminating the conversation, alerting staff or other corrective actions. In my experience, for example, a call will be initiated with a known party, then a second party will join or take over the call. This often occurs when a gang member asserts they are calling a family member, but actually intends to speak to a fellow gang member who takes the place of the family member by using the family member's communication device.

160. Anderson also discloses that after a user's identity is pre-authenticated by the kiosk, and during the transmission of video, the security software (which may be resident on a server as disclosed above in ¶¶130-131) periodically extracts a frame of video and performs facial recognition. "In a first aspect, ... the invention comprises an input-output device including an *image sensor configured to collect facial recognition data proximate to the computer. The sensor device is further configured to communicate the facial recognition data to a security processor.... The security processor is configured to receive the facial recognition*

data and the security parameters associated with the user, and is further configured to at least partially control the operation of the data input device and the data output device in response to the facial recognition data and the security parameters associated with the user.” Ex. 1007, 4:38-56.

161. Anderson discloses that the facial recognition may be used to determine if there is a continued presence of an authorized user’s face, and further discloses that merely detecting the presence of “any face-like object” is sufficient to determine if an authorized face is present. “The various embodiments ... use ... sensors, such as *video cameras*, ... in conjunction with appropriate processing software to ... *to determine whether an authorized user or unauthorized individual is looking at the display. In some exemplary embodiments, **any face-like object is treated as an authorized user.** ... In other embodiments actual recognition is not performed, and the general detection of a “face” is sufficient...*” *Id.*, 8:14-29. So using facial recognition to check for the continued presence of an “authorized” user means that the user has been previously authenticated by Anderson. In a secure facility, parties participating in a video call or video visit “apply” for the privilege. In the application process, or in subsequent use of the system, images of the approved party are captured and retained in the communication system. Those images are then used as a “baseline” for comparison in future communications. Much like TSA has “known travelers”, the communication system maintains the information and images of “known callers” to expedite the authentication process at the initiation and during the ongoing calls.

162. Further, using facial recognition to check for continued presence of any face-like object as an authorized user means that Anderson expressly discloses checking “to determine if a face is present in the frame” as claimed.

163. Anderson also discloses that this frame extraction and facial comparison to monitor for continued presence of a face in the video call is done on

a periodic basis (i.e., “at intervals”). “Whether *facial recognition is used to authenticate initial access to the device ..., facial recognition can still be used to verify continued presence of an authorized individual at the device* as required to maintain privacy of displayed information. ...” *Id.*, 11:21-25. “In ... embodiments, *a check is made at intervals to verify current user identity and continued presence, such as by performing face recognition. The intervals can be kept short, such as several times a second, or done at longer intervals...*” *Id.*, 12:39-43.

164. Anderson also discloses that the face recognition determination is a trigger to enter or leave “privacy mode.” “As depicted in FIG. 17, a video data stream (17000) is fed from a video input device (17010) to an image processor component (17020) of the controller processing thread (17025). *The image processor (17020) prepares individual video frames (17060) for processing by the face tracker (17030)...* *The face tracker (17030) component locates face-like objects in video frames...* *The face tracker (17030) passes the video frame along with face-like object data (17070) it has generated to a face recognizer component (17080).* *The face recognizer component attempts to match face-like objects with previously stored face data so that known individuals can be recognized.* *The face tracker (17030) also provides detected face data (17090) to a face protection logic component (17100) that uses face tracker data (17090) as well as face recognition data (17110) to decide whether there is cause to enable or leave privacy mode, or to generate an alert to the user, ...”* *Id.*, 30:62-31:18. See also, *id.*, 16:14-39.

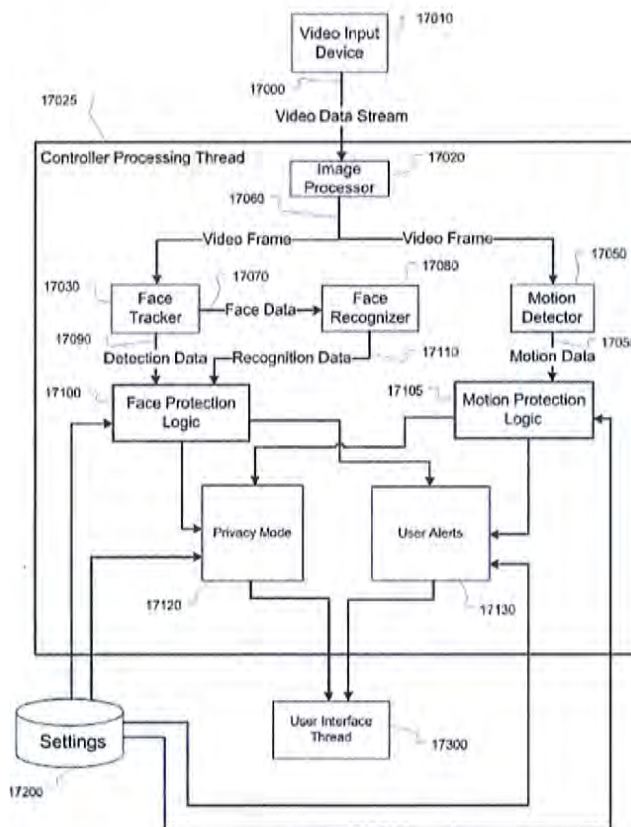


FIGURE 17

Ex. 1007, Fig. 17.

165. Consequently, in the embodiments discussed above in which Anderson (operating on a server) merely monitors for the general detection of “any face-like object,” then “privacy mode” would have obviously been triggered in those embodiments when a face is not detected. If the face recognizer component is unable to confirm the party is the approved and anticipated party, the system moves to “privacy mode”. In practice, this transition protects the content of the conversation and any audio or visual information on the screen. This corrective action is one mechanism to ensure the appropriate parties, and only the appropriate parties, are engaged in the conversation. These actions are similar in function to having a staff member monitor the call directly as the staff member would intervene if parties changed or the context of the conversation changed. This

practice is common in visitation rooms for in-person visitation and in phone calls conducted by offenders.

166. It would have been obvious and predictable for a POSITA that detecting changes in the parties or faces participating in the call as disclosed by Hogg would include detecting the absence of “any” face or face-like object on the call as disclosed by Anderson. While the absence of a face may not absolutely indicate there is a problem, it is a trigger for some evaluation of the call to be conducted. It could indicate illicit activity and the system or a staff member then needs to check to ensure the call is conducted within the parameters set for the call. Both a POSITA and a custody staff member in the secure facility would be very familiar with this practice. Further, it would have been obvious and predictable to a POSITA for Hogg’s facial recognition process to periodically extract a frame of video from the video call to check if a face is present in the frame as taught by Anderson. Again, normal practice in a secure facility is to continually verify that communications are conducted within the established parameters. Consequently, a POSITA would expect the computerized system to reflect this process that is already used for both phone calls and in-person visitation.

- H. **“and the server is further configured to blur the video being transmitted to the destination when the check determines that the face is not present in the frame; and”** (Claim 1.f); **“and the kiosk is further configured to blur video being transmitted to a destination when the check determines that the face is not present in the frame”** (Claim 15.i); **“blurring the video transmission, at the server, to a destination if the check determines that the face is not present in the frame.”** (Claim 22.f); **“and the server is further configured to blur the video being transmitted to the calling party when the check determines that the face is not present in the frame.”** (Claim 24.f)

167. Hogg discloses taking a “responsive action” during a video call if the expected face is not present in the video frame, such as notifying prison personnel,

recording the communication and/or terminating the call. “Call processing system 12 further comprises a call monitoring process 101 that, as discussed further herein, *is operable to monitor communication between caller 11 and called party 13, and based at least in part on the biometric prints detect anomalies occurring in the call, such as a change in the parties participating in the call. ... If determined that an anomaly is detected, such as a change in the parties participating in the call, then a responsive action may be triggered in block 103, such as notifying appropriate personnel, recording the communication (e.g., for future investigative purposes), and/or terminating the call, as examples. While no anomaly is detected, operation advances to block 104 to continue monitoring of the communications between caller 11 and called party 13.*” Ex. 1006, 9:26-44.

168. Additionally, Anderson discloses that when a user’s face is not detected by the facial recognition tracker as discussed above in X.G (i.e., when privacy mode is triggered) the video from the webcam (i.e., video input device) may be obscured (i.e., blocked or replaced by a different data stream). “*In some exemplary embodiments, video input devices are deactivated ... during privacy mode activation. For example, a video chat session or other program that was sending images from the video input device when privacy mode was activated would cease receiving video data from the video input. Alternatively, in some other embodiments, the live video input device data stream is replaced by a pre-arranged data stream, such as an advertisement, “hold message”, music track, screen saver, or other stored or generated data feed. In still other exemplary embodiments, the specific changes made to displayed data, speakers, microphone, video device input stream, or other device aspects depends on factors such as ... whether the user has left the device, the nature of other individuals or devices detected in the vicinity of the device, ...*” Ex. 1007, 16:14-39.

169. Anderson continues, “the ability to restrict or redirect device access as described above is also used to selectively disable particular devices, to alter the functioning of particular devices, *or to substitute other data for the inputs or outputs of specified devices, based on ... **absence of the user***, or the user’s attention to the device. *For example, if the user shifts attention away from the device, the configuration settings can indicate that web camera inputs be blocked, **or that other data**, such as a screen saver, advertisement, hold message, last captured frame prior to the web camera input blockage, or a combination of these or other video or static image data, **be substituted for actual camera input data.*** ... This is useful, for example, when a user is distracted from a video conference by a supervisor entering their office. As the user looks away from the display device, others on the video conference call are not enabled to overhear or see the discussion between the user and the user’s supervisor. When the user looks back to the display device to continue the video conference, the diversion or blockage of the web camera data is halted and normal video input resumed, ...” *Id.*, 26:24-58.

170. One of the several types of video obscuring disclosed by Anderson is “blurring,” and also discloses that blurring is interchangeable with such video replacement. “In some exemplary embodiments the entire display is obscured, such as by pixilation, *Gaussian blurring*, pixel randomization, screen blanking, *activation of a screen saver, substitution of alternative data*, such as a slide show, static image or advertisement, or floating a logo or other image onscreen, opening of extra windows with false or deceptive text or images to distract unauthorized viewers, insertion of random text blocks or images or moving patterns on the screen, or in some other manner make the displayed private data unusable to those viewing it. In devices having a plurality of displays, obscuration can be applied to all, or to a subset of displays, or portions of a plurality of displays.” *Id.*, 16:40-52.

As such, Anderson discloses that video blurring is a type of video obscuration that is interchangeable with use of a screen saver or a replacement video.

171. Anderson also goes into technical detail about how it may implement the various video obscurations, which include blurring the video. “6.12.9 Effect Implementation. The effect implementation permits installation of various modules for generating effects useful for *implementing privacy mode*, such as ... *Gaussian blurring*, etc. ... *Effect modules receive an input image (e.g., an image of the current display device output), performs a transformation of the image, and produce an output image which comprises an obscured version of the original input image*. Examples ... include, ... *Gaussian blur*, ... Each effect module supplies functionality comprising: ...*Effect: invoke the effect. Receives the following input arguments: Source Image: the input image the effect is to be applied to. Destination Image: location to deliver the output image to. Effect Factor: a value useful to control the effect generation. For example, this could be a number representing the speed of a gradual implementation of the effect (e.g., an incremental blur)*.... Ex. 1007, 35:13-55.

172. Thus, Anderson discloses that the transmitted video during a video conference call may be obscured by replacing the transmitted video with alternative data. Later, Anderson such video replacement is a *type* of video obscuring interchangeable with video blurring. In practice, all of the patents (e.g., Hogg and Anderson) are attempting to address the same issue, ensuring the appropriate parties are attending the call and are engaged in the call and/or monitoring for other forms of call anomalies. Should a different person arrive, the appropriate person leave, the appropriate person becomes disengaged (distracted), or some other anomaly is detected on the video call, the communication is then "protected" through various means including replacing the video with a screen-

saver, blurring, pausing, ending the call, notification of staff, etc. The type of protective action is more of an obvious design choice.

173. As such, a POSITA would have been motivated to combine the blurring type of video obscuring disclosed by Anderson as another form of video data replacement “responsive” action, rendering predictable results. A POSITA would consider any of the remediation techniques Hogg and Anderson reasonable and would select the mechanism of remediation based upon the location, they type of “interference” with the expected call, and the risk-based response to the interruption. Hogg and Anderson both list reasonable remediations that could be used within a secure facility. And a POSITA would have found it obvious to obscure/blur the transmitted video in response to detecting an anomaly during a video conference of Hogg as an additional form of protective action disclosed by Anderson.

174. The remedial action (e.g. obscuring) could be accomplished in several ways. For example, when the communication server recognizes the need for remedial action, the server itself could transmit a generic replacement video, a blurred video, no video picture at all for presentation on the client device. In another mechanism, the server could recognize the need for remedial action and send instruction to the client device to simply turn off the display altogether. The specific method of remedial action would be determined in the implementation of the communication system by a POSITA.

175. While positioning user authentication, video monitoring and associated corrective actions, video recording, and other activities on a central server was well known in the art as of April 2011 as discussed above; it was also well known and within the scope of a POSITA that software residing on the kiosks themselves could be performing any or all of these claimed activities. Simply put, rather than have the server software perform the claimed action, the application software

installed in the kiosk could perform that action instead. This is recognized by Anderson, for example. “As will be apparent to those having ordinary skill in the art, the systems, apparatuses, software and methods, provided by the present invention can be adapted to any device that is capable of displaying information under computer control using the disclosure herein.” Ex. 1007, 9:20-38. *See also, id.*, 23:36-24:2, for example, describing the video monitoring of Anderson being performed on a user computing device shown in Fig. 11.

I. “wherein the destination is a device communicating with the server, and the server is configured to authenticate a user of the device.” (Claim 1.g)

176. Hogg discloses that called party 13 is the destination device communicating with the sever, and the server is configured to authenticate a user of the device (called party 13) using pre-stored biometric prints, such as facial recognition, “... *a method comprises determining a biometric print for a party on each authorized side of a call.* As described further herein, the biometric print may comprise any type of biometric data associated with a party *from which the party can be uniquely identified with a high degree of confidence.* ... A biometric print may comprise... face print... In certain embodiments, the parties to a call may be prompted at the outset of the call to take some action to assist in the capture of biometric data from which the biometric print is determined. ...” Ex. 1006, 5:55-6:5. Additionally Hogg discloses, “... *in certain embodiments, a biometric print may have been previously generated for caller 11 and/or called party 13,* and then used by call monitoring process 101 for monitoring a call between such caller 11 and called party 13. *For instance, a voice print may have been generated for caller 11 and/or called party 13 during a previous call, and such voice print may be stored to a computer-readable storage medium and associated with the respective party which it identifies.* For instance, a voice print previously generated for caller

11 may be associated with a personal identification number (PIN) that the caller is required to input when initiating a call. Thus, call processing system may receive the PIN and look-up the previously generated voice print for the caller. Similarly, a voice print previously generated for called party 13 may be associated with the called party's telephone number. Thus, call processing system may receive the telephone number being called by caller 11 and use such number to look-up the previously generated voice print for the called party.” Id., 10:47-11:3

177. Anderson also discloses that the secure facility can have multiple users, all being authenticated by a “centralized security policies” (on a central database server running the central database 9010) to use the video conferencing and disclosed facial authentication/recognition features of Anderson. And, as discussed above in section xxx, “In some cases, *such as in corporate or government use, centralized control of security policies, ... to prevent individual users taking actions that endanger the organization's data security. ... Some exemplary embodiments ...support centralized security policies ... Obtaining data in this way makes required setting and user identification data available to as many devices as required, so that facial recognition is ubiquitously available to any device a user can sign onto. Within a corporate setting or a situation where diverse users in diverse locations need access to the same secure information, this allows many users to have access to data at a plurality of devices without the need to independently configure each user's identification at each individual device. FIG. 9 shows a schematic drawing of a central database (9010) sending user recognition data to a plurality of devices of various types, such as a tablet-based portable computer (9030), a PDA (9050), a desktop computer (9070), and a laptop or netbook computer (9090). The users being recognized (9020, 9040, 9060, and 9080) can be different users....*” Ex. 1006, 21:33-61.

178. Anderson discloses that the security software (which includes the authentication functionality) could reside on a server. “[T]he software can be provided on the web server side, and it would be available to all users (or mostly all depending on browser)....” *Id.*, 17:9-21.

179. Thus, it would have been expected and obvious that the video conferencing disclosed in Hogg or Anderson could be between two users of the same facility and the destination device in the video conference would also require user authentication of each user as disclosed by Anderson. By its nature, video conferencing is intended to connect multiple users at disparate locations to a single communication instance. Each user must be authenticated, whether an offender in a secure facility, a called party outside the facility, another party within the facility, or any combination of parties. That authentication requires logic that compares a known, baseline set of data (image, voice print, password, etc.) to new data submitted during the login/authentication process. Because configuring each potential device independently is unrealistic, a centralized server is used to support the process. As a result, the server can validate many users at the same time, using many devices, potentially of differing types (laptop, tablet, etc.) at the same time while consistently applying the organization's security policies.

- J. “a second kiosk located in a visitation area of the secure facility; and a local server located at the secure facility; the kiosk being configured to transmit the audio and video to the local server when the communications are intended for the second kiosk located in the visitation area; and wherein the local server is configured to record the audio and video and transmit the audio and video to the second kiosk located in the visitation area”**
(Claim 2)

180. Hogg discloses placing a kiosk in an isolated room in the correctional facility: “... a resident of a controlled-environment facility may be required to make a call from a room in which no other resident is present so that the resident is

unable to handoff the call to another resident after the call is authorized/connected.” Ex. 1006, 6:48-53. It would have been obvious and expected to a POSITA that such room disclosed by Hogg could be located in a visitation area of the correctional facility. As staff of secure facilities determine how to support visitation, they consider various scenarios. While face to face, in person visitation is top priority, many jurisdictions consider other mechanisms to address risks or problems in their own facilities. For example, Video visitation can be conducted with visitors entering the secure facility and conducting the session from a private room or specified location within the facility. The offender housed in the facility would be in a separate location in the facility and the technology of the video system clients and servers is used to authenticate, control, and support the communication. This is especially useful in situations where the parties cannot be physically in the same room because of security concerns, sickness, physical limitations, or other issues. These considerations would be a normal process for custody staff and POSITAs in this environment. In fact, staff often used non-contact visiting (in person visiting where the visitor and the offender are separated by a physical barrier of glass or other material) to achieve the same outcomes.

181. For example, Rudolf discloses a video visitation system for prisons that includes a plurality of video visitation kiosks located in various separate locations, including “visitation centers” of a cell block for prisoners. Rudolf’s kiosks located in the cell block visitation centers are the claimed second kiosk located in the claimed visitation area of the secure facility. “Referring ... to FIG. 1... Video visitation communication system includes one or more inmate communication stations 102-110 and one or more visitor communication stations 112-120. ... Similarly, inmate communication stations 102-106 may be located within a visitation center for a first cell block and inmate communication stations 108-110

may be located within a visitation center for a second cell block.” Ex. 1009, [0017].

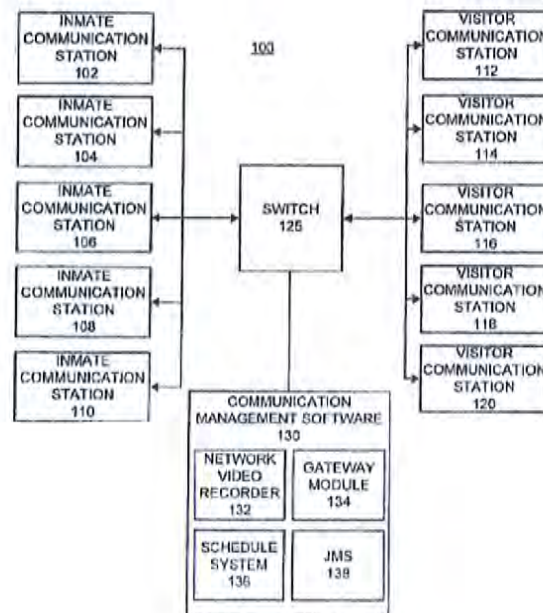


Fig. 1

Ex. 1009, Fig. 1.

182. As discussed above in ¶¶127-129, Hogg discloses that its call processing system 12/12A may be resident on a server. Hogg also discloses that the call processing system 12/12A may be located at the correctional facility. “*Call processing system 12A may be implemented within the controlled environment facility...*” Ex. 1006, 12:34-37. Thus, Hogg discloses that the call processing system 12/12A may be resident on a local server at the secure facility.

183. Shapiro also discloses a local server located at the secure facility. “Inmate Kiosks 613 a-c: Allow inmates to securely interact with *local server 611* over a secure facility network 623.... *The kiosk application ensures that the kiosk is solely used as a window into the local server 611 and local download manager (installed in the server 611)* and only connects to the web for specific pre-approved

functions within the media store (run by server 605), such as listening to song previews from the content provider's server 601....” Ex. 1008, [0133].

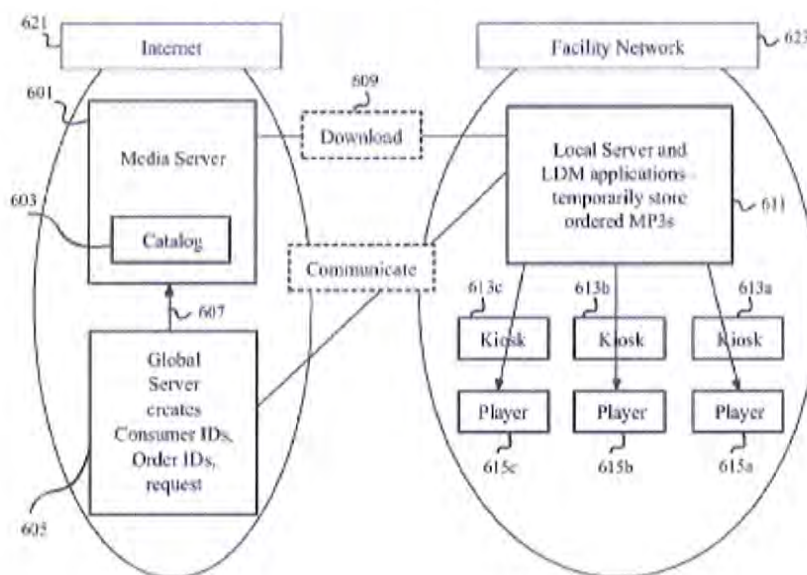


Fig. 6

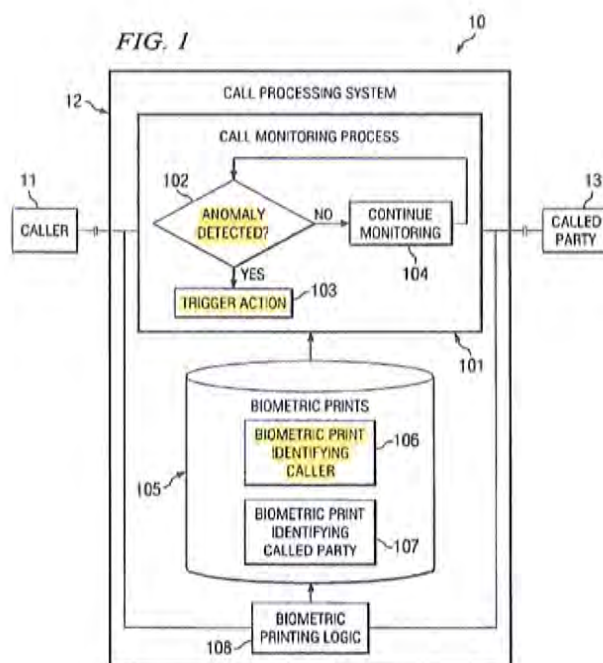
Ex. 1008, Fig. 6.

184. To the extent not completely disclosed by Hogg, it would have been obvious to locate any of the video visitation servers of Hogg, Anderson or Rudolf in a local server located at the secure facility as the applications taught by Shapiro. The location of the servers listed in any of these patents will depend upon the specific locations' physical attributes. Often, servers are located at secure facilities for general computer networks, classrooms content, and radio communications. Secure facilities contain the servers in a physically secure room at the site that is prepared specifically for server-type equipment and provides redundant power, sufficient cooling capacity, fire suppression systems, and a secure area for IT staff to make physical network connections to IT equipment. In some instances, though,

servers are located at a remote facility. This option is explored when a consolidation of servers is preferred for security, cost, support, or other concerns. It would be normal for the IT staff for an organization with secure facilities to consider on-site, or remote sites for the servers.

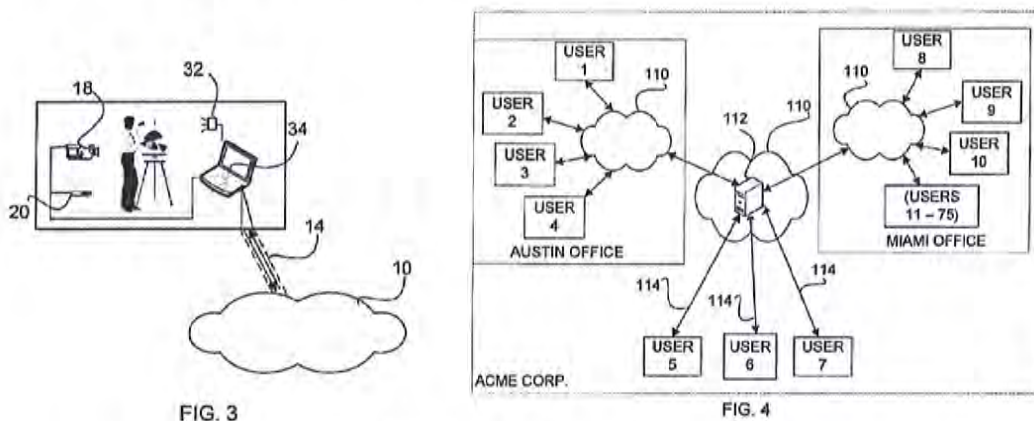
185. For the video visitation, the two parties are connected via a network with a visitation server between the two entities. The network can support a local facility or can span to support a larger organization that has multiple sites. In determining how to configure a video visitation server, a POSITA would consider the best location on the network for locating the server. The server could be placed within the facility which would make the most sense if both communicating parties are at that location, or it could be placed at another physical location that is connected to the organization's network. Bandwidth, security, and supportability all are considerations that would be normal and expected of a POSITA.

186. As discussed above in ¶¶127-129, Hogg also discloses that the call processing system 12/12A is located between a caller 11 and a called party 13, which would have made it expected and/or obvious that any audio/video transmitted between the caller 11 and called party 13 would need to be transmitted to and from the server in-between. No matter where the calling and called parties are located, a "network" is necessary to connect the two parties. This is true in POTS (plain old telephone service) solutions as well as video calling solutions. The capabilities of the network and the involved servers will be different based upon the solution and the security necessary, but in all instances a physical or wireless network is necessary to transmit the voice, video, and or other data from party to party. As such, it would have been expected and/or obvious to a POSITA that the kiosk of Hogg would transmit the audio/video of the video call to the local server of Hogg when the communications are intended for the second kiosk located in the visitation area.



Ex. 1006, Fig. 1.

187. For example, as discussed in ¶¶134-136, Swanson discloses kiosks (user computers 34), configured to transmit and receive audio and video of the communications to and from the server 112 via the network 110. As I noted above, kiosks connect via a network interface to a network which connects both a server and other kiosks. The kiosks transmit and receive the audio and visual information over the network to the server. The server processes the audio and video, which includes saving, validating parties, and other functionality, then passes the appropriate audio and visual information to the second party at the appropriate kiosk.



Ex. 1010, Figs. 3 & 4

188. Rudolf discloses that the kiosks are configured to transmit the audio and video to the server (communication management / administration station 130) when the communications are intended for the second kiosk located in the visitation area for the purpose of allowing the server to record the visitation. As discussed above in ¶¶137-138, Rudolf discloses the communication management 130 may be resident on a server. “According to an alternative embodiment, communication *administration station 130 may include a network video recorder (NVR) 132*. A network video recorder is a digital recording system that receives digital images/video streams over a network and records them on a hard disk in a digital format. Viewing and management of the NVR generally takes place remotely over the network via the administration station 130. Advantageously, *NVR 132 may be coupled to switch 125 and configured to receive audio/video signals from both the inmate communication station and the visitor communication station, such that NVR 132 can create a complete video record of the visitation.*” Ex. 1009, [0021].

189. Rudolf also discloses that the server (administration station 130) gateway module 134 “enables traditional video conferencing” between the communication stations in the visitation areas and those at the court, for example.

“According to yet another exemplary embodiment, administration station 130 may include a gateway module 134. *Gateway module 134 is configured to enable traditional video conferencing between a system 100 communication station and an external videoconferencing system, such as in a public defenders office, a court arraignment hearing, etc.* Gateway 134 may include video conferencing security software such as signal encryption, gateway services, etc.” *Id.*, [0022]. In such a traditional video conferencing arrangement, the kiosk (at the court) would be configured to transmit the audio and video to the local server 130 when the communications are intended for the second kiosk located in the visitation area. From a technical perspective, locating a kiosk at a court is no different than locating a kiosk in a visitation room or other facility. The primary configuration and functionality remains the same, to capture audio and video, and to transmit that information via a network and servers to another party in a different location. Specific functionality for transcription, recording, or other services could be added, the physical implementation would be largely the same.

190. As discussed above in sections X.E and X.J, Hogg discloses that its call processing system 12/12A resident on a local server records the audio/video of a video call and thus would have been obvious and/or expected to a POSITA to record the audio/video of the video call with the second kiosk located in the visitation area. Recording is a long-standing practice for audio calls and would be a natural expectation of custody staff or a POSITA in a secure facility setting. Only privileged calls (legal) are exempt from recording.

191. Rudolf also discloses that the server (administration station 130) may be configured to record audio and video; and also discloses that the server (administration station 130) may transmit the video conference audio/video to a prisoner’s communication station (which may be located in a visitation area as discussed above). “According to an alternative embodiment, communication

administration station 130 may include a network video recorder (NVR) 132. A network video recorder is a digital recording system that receives digital images/video streams over a network and records them on a hard disk in a digital format. Viewing and management of the NVR generally takes place remotely over the network via the administration station 130. Advantageously, NVR 132 may be coupled to switch 125 and configured to receive audio/video signals from both the inmate communication station and the visitor communication station, such that NVR 132 can create a complete video record of the visitation.” Ex. 1009, [0021]. “According to yet another exemplary embodiment, administration station 130 may include a gateway module 134. *Gateway module 134 is configured to enable traditional video conferencing between a system 100 communication station and an external videoconferencing system, such as in a public defenders office, a court arraignment hearing, etc. Gateway 134 may include video conferencing security software such as signal encryption, gateway services, etc.”* *Id.*, [0022].

K. “wherein the server is configured to periodically extract a frame of the video and authenticate a face in the frame against a stored identification image of the user.” (Claim 3)

192. As discussed above, Hogg discloses authenticating a face “print” in the video call against a stored identification image of a user. “Certain embodiments ... further comprise *storing the biometric identification data determined for parties to a call.* ... In this manner, biometric print may be re-used for monitoring future calls involving the respective party...” Ex. 1006, 7:21-28, 14:17-28.

193. Anderson also discloses the server is configured to periodically extract a frame of video and authenticate a face in the frame against a stored identification image of the user. “Once a face-like object is detected, exemplary embodiments can attempt to identify the face-like object as a specific user by means of feature extraction (e.g., face shape, face size, skin color, eye color, eyebrows, eye shape,

nose shape, mouth shape, hair color, glasses, estimated angle of face to the screen, etc.) and comparison with a file, database or other secure information source containing identification information for one or more users.” Ex. 1007, 10:57-65.
“As depicted in FIG. 17, a video data stream (17000) is fed from a video input device (17010) to an image processor component (17020) *The image processor (17020) prepares individual video frames (17060) for processing by the face tracker (17030), and motion detector (17050) components. ... The face recognizer component attempts to match face-like objects with previously stored face data so that known individuals can be recognized. ...*” *Id.*, 30:62-31:14

194. As discussed in section X.G, Anderson also discloses that the facial recognition on the extracted frames is done periodically (at intervals). As discussed above in section X.C, Anderson’s security routines can be resident on a server.

195. Thus, to the extent not completely disclosed by Hogg, the combination of Hogg and Anderson shows it would have been obvious to a POSITA that the server is configured to periodically extract a frame of the video and authenticate a face in the frame against a stored identification image of the user, rendering predictable results. The problem of authenticating users is the same problem that has existed in telephone calls for some time. In a video call, it would be reasonable to extract a picture or photo from the video stream to compare to a known photo or video extract to ensure the parties participating in the call are the expected parties, throughout the call.

- L. **“wherein during a singular communications session, the kiosk is configured to periodically record a frame of video and transmit the frame to the server, and wherein the server processor authenticates a face in the frame against a stored identification image of the user.” (Claim 4)**

196. As discussed in section X.K, Hogg and Anderson disclose the server is configured to periodically extract a frame of the video and transmit the frame to a

server to authenticate a face in the frame against a stored identification image of the user. The kiosks would have obviously and necessarily recorded these frames, at least temporarily, as part of this step prior to transmitting to the server. The act of capturing an image, for any purpose, is an act of recording the image. The kiosk would necessarily be (or obviously would have been) capture the image and sound information with a camera and microphone embedded in the device which facilitates the ability to store the data, whether on the kiosk device, or on the server which is located on the communications network. As discussed in sections X.H and X.G, Hogg's and Anderson's face authentication and security processes are performed during a singular communications session, such as a video conference (i.e., a video chat session). As discussed in section X.E Hogg, Anderson and Rudolf disclose recording the video conference.

197. As discussed in section X.G, Anderson discloses periodically (i.e., "at intervals") performing the facial recognition against a stored identification image. Additionally, Hogg discloses periodically recording a frame of video, for example, when an anomaly is detected in the video conference. *See, e.g., Ex. 1006, 9:26-44. "If ... an anomaly is detected, such as a change in the parties participating in the call, then a responsive action may be triggered in block 103, such as ... recording the communication (e.g., for future investigative purposes)".* Thus, the combination of Hogg, Anderson and Rudolf show it would have been obvious to a POSITA for the kiosk to periodically record a frame of video and transmit the frame to the server during a singular communications session, where the server processor authenticates a face in the frame against a stored identification image of the user. Each of Hogg and Anderson discloses the functionality of capturing an image or portion of a call, then evaluating that information against information that was previously used to identify the known party. For practical use in a secure facility,

this process would need to occur during the call, and as close to "real time" as possible using the type and size of the technology implemented.

M. **"wherein the kiosk is configured to accept messages input by the user after the user has logged on and transmit the messages to the server, and the server is configured to provide a third party access to the messages."** (Claim 5)

198. Hogg discloses that the kiosks may be configured to accept handwritten messages input by the pre-authorized (i.e., logged-on) user (that have been authenticated as discussed above in section X.F) as a form of a "call" so that they are transferred to the server (see section X.D above), and that the server is configured to provide a third party (e.g., a called party or an investigator) access to the call record that includes the handwritten messages (as biometric information). "Embodiments of the present invention can be applied for monitoring various types of calls. ... Thus, a "call" is not limited to telephony calls, but also encompasses various other types of communication. ... *As another example, a handwritten communication, such as a **handwritten message input to a computer device, such as a personal digital assistant (PDA) or laptop computer, and communicated via a communication network may be analyzed using known handwriting analysis techniques for performing biometric identification of the writer.** ...*" Ex. 1006, 5:29-54. "*As another example, ... the communication between caller 11 and called party 13 comprises **handwritten communication.** For instance, various computer devices, such as tablet PCs, are available that accept handwritten input, such as a pad that enables a user to provide handwritten input using a stylus. **Such handwritten messages may then be communicated, e.g. via a packet-switched network, between a called party 13 and a caller 11.** In such case, biometric printing logic 108 may generate handwriting-based biometric prints, such as a handwriting print for use in recognizing an individual's handwriting. *Thereafter, the handwritten communications between caller 11 and called party 13 may be**

monitored and compared with the generated handwriting-based biometric prints to, for example, detect changes in the parties participating on the call.” Id., 10:15-29. “Certain embodiments of the present invention further comprise storing the biometric identification data determined for parties to a call. ... Thus, if an investigator desires to later retrieve the call record and review the parties participating on the call, including the biometric identification performed during the call, he can do so via the call's stored record. ...” Id., 14:17-44.

199. Shapiro discloses the kiosks are configured to accept messages input by the user after the user has logged on and transmit the messages to the server, and the server is configured to provide a third party access to the messages for screening the messages. Shapiro discloses “... an inmate may use a kiosk or digital content player to create outbound messages directed to family members, for example, and distributed through use of the communications architecture of the present invention.” Ex. 1008, [0040]. Shapiro continues, “[b]efore sending an initial letter, a writer first opens an account by filling out an input form that requires data, such as a username, a password and an optional e-mail address.” *Id.*, [0070]. Shapiro continues, “[t]he inmate letters are stored on the server 255. The status of each letter is also stored. Such status indicates whether the letter has already been downloaded and read, whether the letter should be held for review and which keywords may have been detected.” *Id.*, [0098]. Shapiro continues, “[c]orrection authorities read inmate mail... correction authorities are alerted if inmate letters contain prohibited keywords. Third, correction authorities can read letters and indicate in the letter table that a particular letter has been reviewed and if held for review subsequently released to the inmate. ...” *Id.*, [0113].

200. It would have been obvious to a POSITA to implement Shapiro’s message writing, routing and monitoring functionality with Hogg’s system, rendering predictable results. A keyboard, pad that accepts handwritten notes,

scanner to capture paper notes, and microphones are all examples of "input" devices that can capture the information provided by a user of a kiosk. While the mechanisms of comparing each type of information are different, the intent of each comparison is the same, to validate that the submitting party is the expected party by comparing to previously captured or known information. As an IT staff member in a secured facility, this need is well known and a reasonable expectation no matter the type of communication (data) input. With access to these prior art patents (including Hogg and Shapiro), it would have been obvious to combine any or all of these capabilities as dictated by the type of data capture device used.

- N. **"wherein the kiosk is configured to provide the user with at least two of: access to audio, video, and text of educational material stored on the server and/or the kiosk, access to audio, video, and text of religious material stored on the server and/or the kiosk, and the ability to order items from a list of commissary items."** (Claim 7); **"wherein the kiosk provides the user with at least one of: access to audio, video, and text of educational material; access to audio, video, and text of religious material; the ability to order items from a list of commissary items; the ability to reserve times for using the kiosk; and the ability to send text messages to third parties"** (Claim 16)

201. Shapiro discloses kiosks configured to provide the user with: access to digital content in the form of audio (music or songs), video (movies) and text (ebooks); and the ability to order items from a list of commissary items (i.e., physical items) from a content server ("Digital Fulfillment Server," See Fig. 3 and/or media server 601). "Another embodiment of the present invention *includes the delivery of digital content, such as music, to inmates. ... FIG. 3 is a basic schematic diagram 10 of a digital content store system 12 implemented between a digital content store 14 and a client machine 16. A user USR at a client machine 16 may access the digital content store 14 through a store link and account module 38, such as through a user interface 103 (FIG. 4). The store module 38 is typically*

associated with a selectable inventory 36 of assets (e.g., songs), which are typically accessible 42, 44, upon purchase ...” Ex. 1008, [0114].

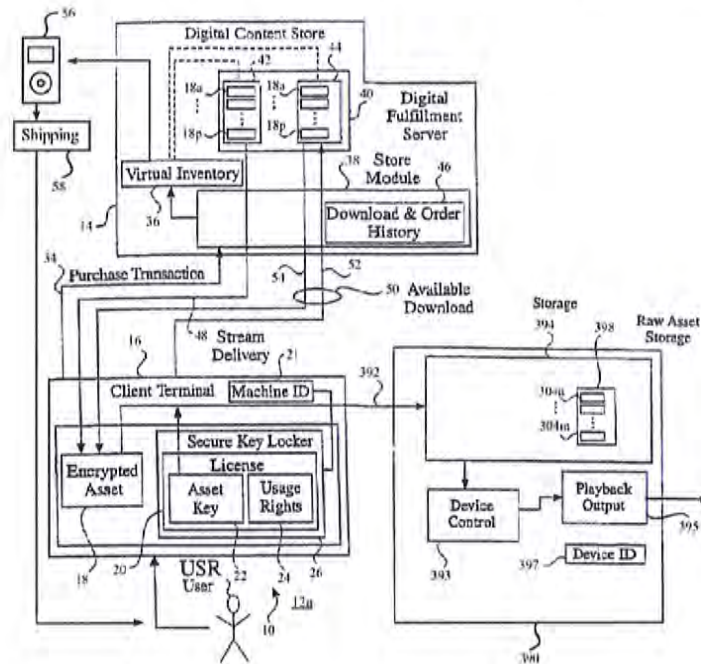


Fig. 3

Ex. 1008, Fig. 3.

202. Shapiro continues, “... the user USR may also *use the system to purchase physical inventory of content 56, ... Upon purchase 34, some system embodiments comprise both delivery of physical content 56, along with downloading of encrypted digital content 18, whereby the intended user USR can quickly access content 18, such as songs, movies, games, or other content 18.” Id., [0116]. “The system and method of the present invention allow inmates to buy digital media, including individual songs, albums and eBooks, from an Inmate Kiosk and download it to a personal portable player of digital content (the “Player”) ...” Id., [0131]. “Global Server 605: Administers services to an online*

store running in server 601 and eCommerce over the Internet 621.” *Id.*, [0132]. See also, *id.*, [0138].

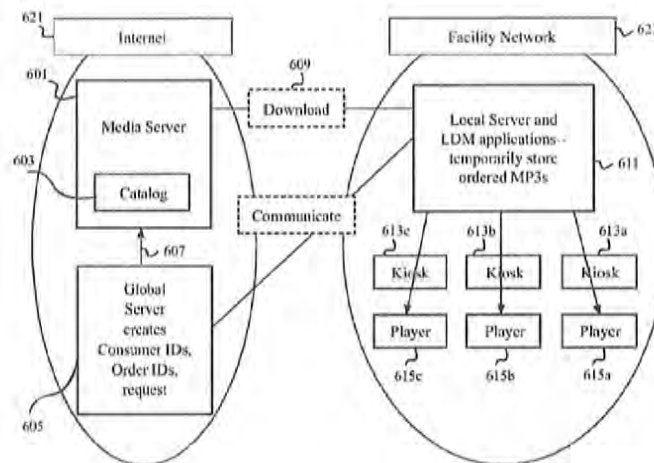


Fig. 6

Ex. 1008, Fig. 6.

203. It would have been obvious to a POSITA to provide the digital media and physical item store on a server as disclosed by Shapiro as an additional feature that the kiosks of Hogg, Anderson, and/or Rudolf, similar to Shapiro's systems deploying a combination of e-messaging and content store features as disclosed – rendering predictable results. With the introduction of kiosks, servers, and the connecting networks in the secured facility, it would be natural to use those capabilities to both improve the services provided to residents (inmates) and to also minimize the labor required by institution staff in fulfilling requests. By implementing "self-service" processes on the technology, desired items are delivered to the resident (inmate) faster, the risk of contraband being delivered to an inmate is lowered, and the labor of staff members is reduced which allows staff to focus more on safety and security measures. Automation of the processes also

increases the consistency with which processes are conducted and evaluated, and introduces more data about the process which can be evaluated for security risks, delays that can be minimized, patterns, inventory management, etc. In addition, combining the processes into the single kiosk lessens the amount of physical space required within the secure facility. Space is often a limiting factor in deciding which services can be provided in a secure facility.

204. Further, to the extent that the specific subject matter of the digital content carries any patentable weight, it would have been well known and obvious in prison settings that digital audio, video or ebooks would have obviously been in the form of educational or religious materials. While digital audio, video, or ebooks can take on the form of entertainment, creative outlet, or other forms, educational material and religious materials are long-known and expected materials in a prison setting. Education is a responsibility of correctional organizations and depending on the age and risk classification of the offender, can be required by statute. In some instances, a prison system may even be part of, or form its own school district or system. In addition, religious materials are a known and expected right in the prison industry. Religious freedom is an important aspect in the custodial setting and religious material is normally included in the listings of materials considered reasonable "inmate property" in correctional regulations.

205. Further, to the extent that the source of the physical items carries any patentable weight, it is also well known that sale of physical items in the prison setting are obviously from a commissary. While it is possible for some materials to be introduced by family, prison support or advocacy groups, or other means, most materials are introduced through the commissary process. And, digital media delivered to kiosks, no matter the source, would be evaluated and approved by correctional officials before being introduced into the electronic system. The electronic commissary system performs the function of fulfilling orders for

"purchased" items and tracking the "loan" of items that are temporary or free in the setting (e.g. a library ebook). The physical commissary has been a long-standing method for offenders to obtain specific types of inmate property or items deemed appropriate by the correctional officials. Items can include anything from snack foods, to some medications (e.g. aspirin). An order/fulfilment process is established that could take the form of a "walk-up window" on an exercise yard, or a paper request/order form collected by staff with items then delivered to a cell (or room) at a later time.

- O. **"wherein the log in information is a personal identification number"** (Claim 9); **"wherein the personal log in information is a personal identification number"** (Claim 17)

206. Hogg discloses that the log in information includes a personal identification number (PIN). "... For instance, a voice print previously generated for caller 11 may be associated with a personal identification number (PIN) that the caller is required to input when initiating a call. *Thus, call processing system may receive the PIN and look-up the previously generated voice print for the caller. ...*" Ex. 1006, 10:47-11:3.

207. Anderson also discloses the use of passwords as log-in information. "... *Recognition of individuals by means of face recognition can be combined with additional authentication means, such as passwords, shared tokens, biometrics or other well known techniques, or used alone. ...*" Ex. 1007, 10:54-11:9. *See also, id.*, 11:52-56. Passwords are synonymous with personal identification numbers. The ability of identifying any individual is necessarily dependent upon the individual provided some sort of identifying information. This could be as simple as a PIN known only to them, a combination of username and password, an offender ID number, a fingerprint, or other items. Each mechanism fulfills the same need and could be used to "authorize" the use of a kiosk, a purchase, or other transaction.

The number and type of identification steps would be dependent upon the type of transaction. For example, a PIN is a simple, low complexity mechanism for authorizing low-risk activities (placing a call), but a username and password may be required for higher-risk activities like bank transactions.

208. To the extent not completely disclosed by Hogg, the combination of Hogg and Anderson show that it would have been obvious to a POSITA that the log in information is a PIN number, with predictable results. The need to identify a party is the underlying function that must be fulfilled and that need is well known in the correctional/secure facility industry.

- P. “wherein the biometric verification comprises a facial authentication via the camera” (Claim 10); “wherein the biometric verification comprises a facial authentication of an image captured by the camera” (Claim 18)**

209. As discussed above in section X.F, Hogg and Anderson disclose that the biometric verification comprises facial authentication via the camera (webcam).

- Q. “wherein the biometric verification comprises a voice authentication via the microphone” (Claim 11); “wherein the biometric verification comprises a voice authentication of an audible phrase recorded using the microphone.” (Claim 19)**

210. Hogg discloses the biometric verification includes voice authentication via an audible phrase spoken into the microphone. Hogg discloses, “... a method comprises *determining a biometric print for a party on each authorized side of a call. ... the biometric print may comprise any type of biometric data associated with a party from which the party can be uniquely identified with a high degree of confidence. ... A biometric print may comprise, as examples, a voice print, face print, ... and/or the like. ... For instance, the parties may each be prompted to speak their names so that audio data can be obtained from which a voice print can be determined for each party.*” Ex. 1006, 5:55-6:5. “[A] biometric print may

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

have been previously generated for caller 11 and/or called party 13, and then used by call monitoring process 101 for monitoring a call between such caller 11 and called party 13. For instance, a voice print may have been generated for caller 11 and/or called party 13 during a previous call, and such voice print may be stored to a computer-readable storage medium and associated with the respective party which it identifies. For instance, a voice print previously generated for caller 11 may be associated with a personal identification number (PIN) that the caller is required to input when initiating a call. ...” Id., 10:47-11:3. It would have been obvious and expected to a POSITA that such voice print data would be recorded via the kiosk’s microphone. No matter the type of communication, an IT professional (POSITA) or a correctional staff member would expect the communication device (kiosk) to capture data for use in comparison to known information to establish/confirm the identity of a party. In the case of an audio sample, it would be reasonable and expected that a microphone within the device provide the capability to capture the voice input for comparison. This same capability has existed in telephones for that type of communication for many years and would be expected in any new device.

- R. “wherein the server is configured to detect the presence of a second face in the video frame and, while the presence of the second face is detected, the kiosk is configured to blur the video” (Claim 12); “detecting the presence of a second face in the video frame and, while the presence of the second face is detected, blurring the video transmission, at the server, to the destination” (Claim 23); “wherein the server is configured to detect the presence of a second face in the video frame and, while the presence of the second face is detected, the server is configured to blur the video being transmitted to the calling party” (Claim 28); “wherein the kiosk is configured to detect the presence of a second face in the video frame and, while the presence of the second face is detected, the kiosk is configured to blur the video” (Claim 20)**

211. Hogg discloses that its server is configured to detect the presence of a new unauthorized face (i.e., a second face) joining the call as an example anomaly that would require corrective action as discussed above. “..., *face prints are obtained for parties* that are authorized to participate on a call. The *call is then monitored and video communication of the call (e.g., of a video conference call) is used for comparison with the face prints* of the authorized parties to detect changes in the parties participating on the call, *such as a new, unauthorized party joining the call*. Thus, embodiments of the present invention advantageously enable a call processing system to monitor calls and detect anomalies occurring during the calls, such as three-way calling, a handoff of a call from one party to another, etc.” Ex. 1006, 8:43-50.

212. Further, Anderson discloses the server is configured to detect the presence of a second face (e.g., a third party behind the user or an unauthorized face) in the video frame and initiate privacy mode in that instance. Anderson discloses, “... *facial recognition data includes image data relevant to determining the presence of a third party in a region behind the user*... In other embodiments in which the security processor is configured to provide a warning upon *detecting the presence of a third party in the region*, the security processor is configured to

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

modify the operation of the video display upon detecting the presence of a third party in the region. ... Ex. 1007, 4:57-5:12. *See also, id.*, 15:26-33. “Alerting the current user to the presence of additional or unauthorized viewers can be done in a number of different ways. For example, the video input device data feed can be shown on the device display, whether in full-screen mode, which might be disruptive to the current user's work, but would have the beneficial side-effect of *obscuring the sensitive data*, or in a smaller window that takes up only a portion of the display area. ...” *Id.*, 19:63-20:6. “FIGS. 8A and 8B depict an exemplary video input device data feed (8010) with an authorized current user (8020) and an unauthorized, or unrecognized additional face-like object (8040). ... privacy mode is activated according to the security policy of this example, and the sensitive text (8120) and graphic data (8130) being displayed are obscured.” *Id.*, 21:14-23.



FIGURE 8A

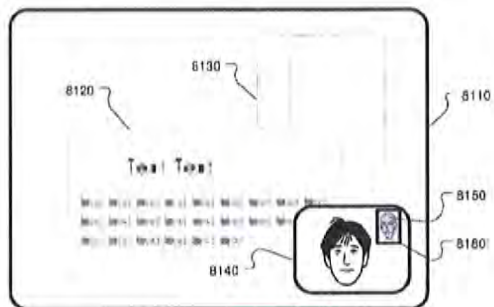


FIGURE 8B

Ex. 1007, Figs. 8A & 8B

213. As discussed above in section X.H, Hogg and Anderson disclose and/or render it obvious to a POSITA to blur the input device (camera) feed on a video call when an anomaly is detected and/or privacy mode is triggered.

- S. **“wherein the server is configured to record video in a tele-medical session mode wherein the blurring the video being transmitted to the destination is not performed when the check determines that the face is not present in the frame” (Claim 13); “wherein the kiosk is configured to record video in a tele-medical session mode wherein the blurring the video being transmitted to the destination is not performed when the check determines that the face is not present in the frame” (Claim 21)**

214. Anderson discloses that “privacy mode” activation may be disabled where presence of the user’s face is not required. “In some exemplary embodiments, and where this is permitted by applicable security policies, the user can temporarily *disable the features activation of privacy mode* when giving presentations or *performing other tasks where the current user's face is not visible to the attention sensor, but privacy of screen data is not required.*” Ex. 1007, 17:65 to 18:3.

215. While Anderson does not state that this would be during a tele-medical session mode, a POSITA would have understood and/or found it obvious that a user may need to transmit video of other anatomy during a tele-medical visit. Telemedicine is a good example of a video conversation that would not require the “normal” communication protections. In fact, telemedicine communications may not be recorded in an effort to protect the confidential medical information of the patient. In an example, if a patient is complaining of a rash on their extremities, it would be normal and expected that the specific extremity, an arm for example, would be placed in front of the camera, blocking the view of the face. Because that would be an expected and reasonable practice in this type of video call, the normal security and privacy settings would need to be disabled during this type of

conversation. The same need may exist in video calls conducted with legal staff when discussing injuries that occur while housed in a secured facility.

216. For example, Swanson discloses that video conferencing could be tele-medical sessions and the participating doctors may need to review items other than a caller's face, such as by viewing X-rays. "Applications for use of video communications sessions ... include ... medical consultation... In a medical consultation application, doctor specialists ... can participate in the diagnosis of a particular case. X-rays can be viewed by all..." Ex. 1010, 7:48-64.

T. the kiosk ... "provides access to internet web pages via a web proxy, and" (Claim 15h)

217. Shapiro discloses that its inmate kiosks include ability to connect to the web through a web proxy (kiosk application, local server 611 or local server 1912). "Inmate Kiosks 613 a-c: ... *The kiosk application ensures that the kiosk is solely used as a window into the local server 611 and local download manager (installed in the server 611) and only connects to the web for specific pre-approved functions within the media store (run by server 605)...*" Ex. 1008, [0133].

218. Microsoft Computer Dictionary defines "proxy" as "A computer (or software that runs on it) that acts as a barrier between a network and the Internet by presenting only a single network address to external sites. By acting as a go-between representing all internal computers, the proxy protects network identities while still providing access to the Internet." See. Ex. 1018.

219. It would have been obvious as taught by Shapiro to limit Hogg's, Anderson's, etc. access to internet web pages via a web proxy. All of the technology introduced into a secure facility requires security precautions to ensure the appropriate use of the technology. A computer or kiosk used for communication should not be usable as a general web-browser or for another type of unapproved communication. The proxy server described in Shapiro, for

example, performs the function of ensuring that the kiosks can communicate only with the specified (configured) servers and only for specific functionality. In addition, this proxy eliminates the ability for anyone (or any device) outside the secure facility to determine the specific kiosk or device that initiated a request, search, transaction, or other process that is allowed on the internet. This effectively builds a "closed" network that is tightly controlled and monitored by the staff of the secure facility. For example, offenders in a prison may attempt to use a kiosk intended for video calls with family members for searching the internet for instructions about building weapons, for attempting communication with unapproved parties, or for illicit banking transactions.

220. For each of Sections X.E through X.T, above, Anderson discloses that the systems for practicing such claim elements may optionally reside on "personal computers" (i.e., kiosks) in addition to servers. Ex. 1007, 9:20-38. *See also, id.*, 23:36-24:2 (*e.g.*, describing the video monitoring of Anderson being performed on a user computing device shown in Fig. 11).

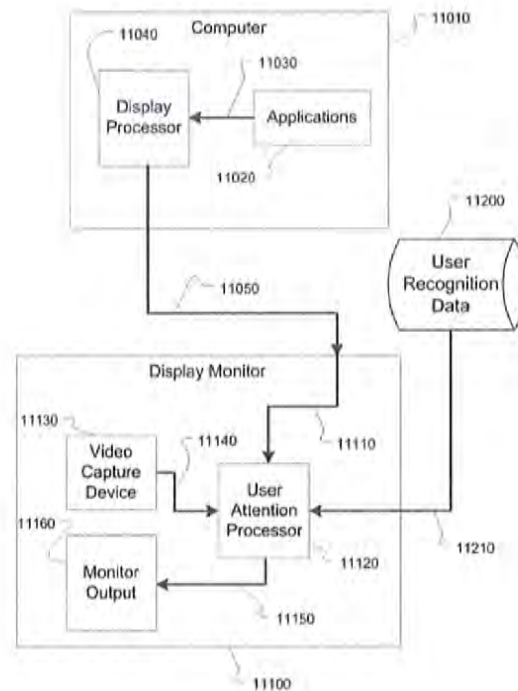


FIGURE 11

Ex. 1007, Fig. 11.

- U. **“wherein the server is configured to receive a communications request from the device of the outside party and, in response to the received communications request, identify a kiosk in a vicinity of a requested party and transmit a message to the kiosk,”** (claim 24); **“wherein the server identifies the kiosk in the vicinity of the requesting party by referencing a resident schedule that is stored on a computer readable medium of the server”** (Claim 26);

221. Hogg discloses the ability to track the location of inmates within a prison, and where the call processing system 12/12A may utilize that information as part of its anomaly monitoring processes. “RFID may be used to track the location of residents within a controlled-environment facility... [S]uch location information may be supplied to a call processing system ...” Ex. 1006, 13:48-59.

222. Shapiro Fig. 6 also shows a plurality of inmate kiosks 613a-c at a correction facility. *See also*, ¶¶118, 183. Shapiro also discloses that each inmate includes a location field associated with the inmate ID in the server database, which are used for routing messages from outside parties to inmates. “FIG. 2 illustrates ... The inventive system and method routes letters and other correspondence by using, for example, a table in database 257 that indicates the inmate's name ... and facility location code...” Ex. 1008, [0037]. “The correction system facility code uniquely identifies the correction facility within the correction system that holds that particular inmate. This facility code thereby determines which letters will be placed into that facility's mail file during the next mail delivery (or download).” *Id.*, [0054].

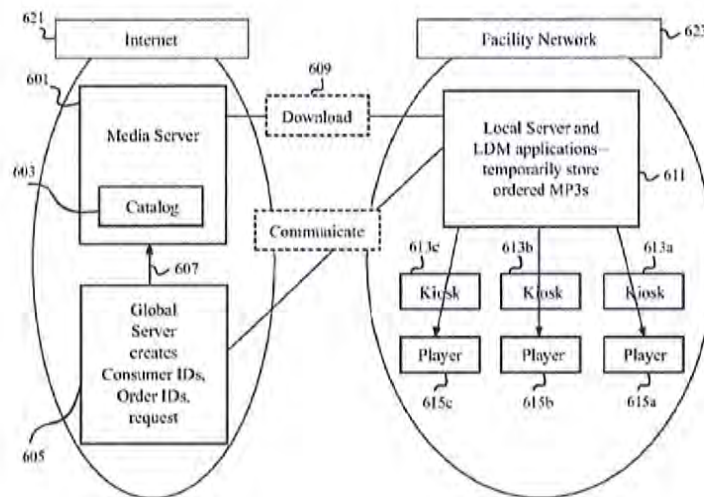


Fig. 6

Ex. 1008, Fig. 6.

223. It would have been obvious to locate the vicinity of an inmate as taught by Hogg or Shapiro for routing electronic messaging to a kiosk using that facility

location code. Accountability within a secure facility is and has always been a top priority. Whether for safety of the offenders and staff, responding to an emergency, or simply ensuring students are in the appropriate classroom, some system of tracing the location of offenders is always in use. That could include electronic mechanisms like RFID (remote frequency identification) where sensors throughout the facility detect the location and movement of a party or item, simple paper sign in sheets, or a multitude of other means, accountability is a critical and necessary function in the environment. Consequently, the processes of Hogg and Shapiro would be normal and expected to enable the delivery of messaging to the offender. Often, though, the locations where an offender could receive the message would be constrained. For example, it may not be permissible to deliver a message that interrupts the time an offender is intended to be in a classroom, even if the capability exists.

224. Cree also discloses an inmate messaging system that delivers a message from an outside party to a prisoner by automatically dialing the kiosk in the cell block the prisoner is located; and also delivers a notification to the inmate that a message is available. “An inmate messaging system and method for notifying an inmate in a prison facility of messages received from a caller outside the prison facility.” Ex. 1011, Abstract. Cree continues, “... the system 130 delivers 374 the call request by automatically dialing the cell block telephone number in the cell block where the inmate is housed.” *Id.*, 10:19-22. “If 386 any messages are pending, the system 130 will announce 396 a list of the messages over the cell block telephone 150.” *Id.*, 10:51-53.

225. It would have been obvious to modify the combination of Hogg, Anderson and Shapiro to use the prisoner location disclosed by Hogg and/or Shapiro for automatic messaging of kiosks where the prisoner is located and sending a notification of such message as disclosed by Cree. The ability to deliver

a message, commissary item, package, mail, or any item to a resident/offender in a secure facility is dependent on knowing both where the party is and where they should be. Any custody staff member or POSITA would anticipate that need to enable the delivery of items or notification of items or processes. For example, the technology could be used to simply remind an offender of the time and location of a scheduled appointment with a job counselor, or the delivery of items ordered from a commissary.

226. Rudolf discloses that it would have been obvious that automated selection (e.g., by the server) of a visitation kiosk for a video visit may be based on a predefined schedule of the prisoner. "The visitor communication station may be selected based on a pre-defined schedule, may be selected automatically by system 100 using scheduling system 136, ..." Ex. 1009, [0042]. As discussed above, the location information of an offender is necessary to ensure the safety and security of the facility, and to ensure all offenders and staff are accounted for in the case of an emergency. To enable those needs, prisons have schedules and limitations on where they can be. Depending upon the risk level (e.g. high security vs. low security) of an offender, some are allowed movement within a facility only when accompanied by a custody staff member while other offenders are provided a "hall pass" that allows them to transition from one location to another unaccompanied. No matter the mechanism used, thought, the anticipated and actual locations of offenders are known and compared to ensure the daily activities are in concert with the plan.

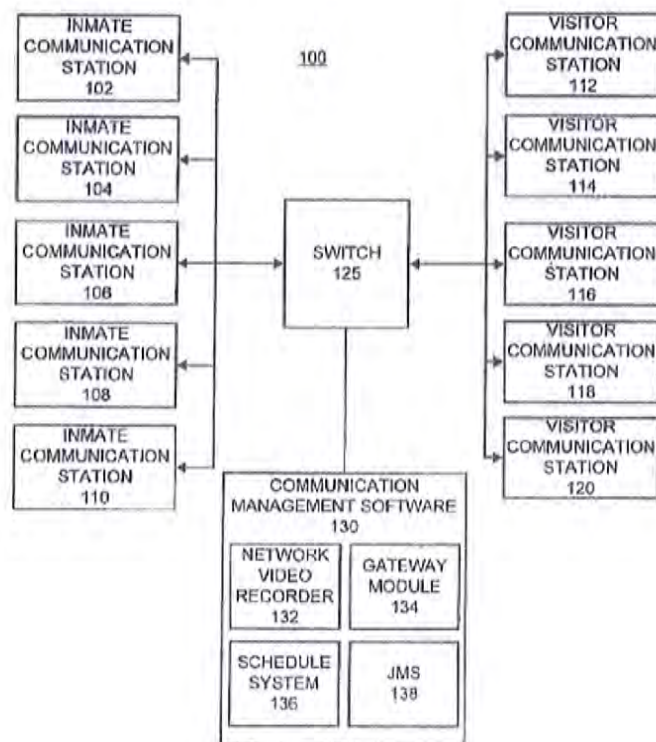


Fig. 1

Ex. 1009, Fig. 1.

- V. “wherein the kiosk is configured to receive the message, and, upon receipt of the message, display an incoming communications request message and initiate a login procedure,” (Claim 24);
“wherein the kiosk is configured to receive text-based messages from a server, and to display a notification of an available text-based message on an idle screen of the kiosk” (Claim 8)

227. As discussed in ¶224, Cree discloses that messages are directed to the cell block in which the inmate is located and provides a notice to the inmate of an incoming message. Cree also discloses that, if the inmate wishes to accept the message, the kiosk will initiate a log-in procedure requesting the inmate’s PIN. “If 390 the inmate selects a messaging function from the menu of options, system 130 prompts the inmate to enter 392 an account number and PIN.” Ex. 1011, 11:10-12.

228. Swink discloses that it would have been obvious to display a notice of an incoming communication request message on a display screen of a kiosk (mobile device), which may be in a locked (i.e., idle) state. For example Swink discloses, "...the communication device ... can overlay and display information relating to a notification (e.g., notification of an incoming phone call, notification of an incoming text message (e.g., short message service (SMS) message... instant message (IM), ..., etc.), ... on the display screen of the UI, for example, when the communication device is in the locked state, or when the communication device is using an application ..." Ex. 1012, [0015].

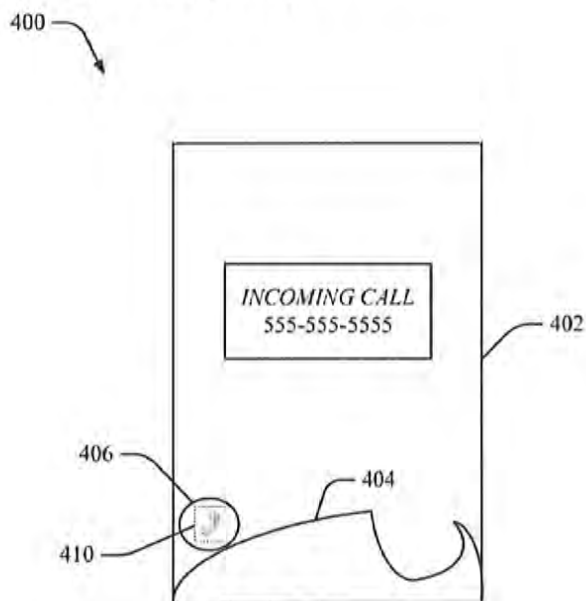


FIG. 4

Ex. 1012, Fig. 4.

W. “wherein the kiosk is configured to play an alert tone or audio message upon receiving the message.” (Claim 27)

229. It is well known for laptops, PDAs and mobile phone devices of the prior art to play an alert tone or audio message upon the device receiving a message. As a well-known example, America Online was famous for its audio message “You Have Mail” with the delivery of electronic messages in the late 1990s. *See, e.g.*, <https://www.latimes.com/archives/la-xpm-1999-jan-05-fi-60434-story.html>. This functionality simply alerts party to draw their attention to the message. Without that alert, the party would need to proactively check the device to discover the existence of a message. The “alert”, then, allows messages to be received in a timely manner. Anderson discloses “sounding an alert tone” as a means for “alerting the current user to the presence of unauthorized viewers.” Anderson 20:16-25. Swink discloses that the communication device may include “speakers, vibration generator... that can be used to facilitate presentation of information to a communication device user.” Ex. 1012, [0152]. It would have been obvious to use such disclosed audio alerts to alert a user of an incoming message. The use of an audio tone would be a reasonable and expected alert in many environments. There may be a few, though, that require a visual clue for people with hearing impairments, or working in environments in which there is a large amount of ambient noise.

XI. MOTIVATIONS TO COMBINE THE TEACHINGS OF THE PRIOR ART AND REASONABLE EXPECTATIONS OF SUCCESS

230. From small jurisdictional sites (e.g. small county jails) to moderate sites (e.g. state hospitals), to extremely large sites (e.g. state prisons), secure facilities share some primary objectives, safety and security. No matter whether the mission is health care, education, general operations, or rehabilitation, unless a site is safe and secure for both the staff and the residents/inmates/patients, the primary

mission cannot be accomplished. In these secured environments, jurisdictions need to provide digital education, communication, and commerce tools to enhance a jurisdiction's ability to provide effective services for the staff and to residents/inmates/patients. While improving efficiency and effectiveness, those same tools can also improve security and safety for all involved through improved access by offenders, reduced travel by parties outside the environments, and both monitored and recorded interactions. In addition, staff need the ability to know when transactions are compromised, whether by electronic or physical means.

231. With that in mind, Hogg, Anderson, Shapiro, Rudolf and Cree are all clearly in the same field of endeavor, electronic communications services for secure environments. Hogg discloses, “[e]mbodiments ... have particular applicability within controlled-environment facilities for monitoring the calling activities between a resident and other parties.” Ex. 1006, 4:67-5:2. Anderson discloses, “[t]he technology herein has applications in the areas of data processing, portable computing, computer-based communications, computer security, and data privacy maintenance”. Ex. 1007, 3:33-36. Shapiro discloses, “[t]he present invention relates to the field of electronic communications. Specifically, ... to the delivery and access of electronic data by individuals in a restrained environment, such as correctional facility.” Ex. 1008, [0002] Rudolf discloses, “[t]his invention relates generally to systems and methods for implementing video visitation where the only contact between individuals is through a video and audio connection.” Ex., 1009, [0001]. And Cree discloses, the “invention relates to the field of telecommunications and, more particularly, to an inmate messaging system ... for notifying an inmate ... of messages received from a caller outside the prison facility.” Ex. 1011, 1:6-10. As such, a POSITA would be motivated to combine the teachings of all of Hogg, Anderson, Shapiro and Rudolf as they all pertain to electronic communications in secure environments.

232. While Anderson does not disclose use in prisons, Anderson discloses use in “government, ..., and military applications...” Ex. 1007, 4:28-37, 9:20-38. These environments have similar security concerns as compared to prisons. While Hogg, Shapiro, Rudolf and Cree discuss custodial environments, the need in a military or other high security environment (e.g. first responder, financial, medical) is very similar. The needs to protect the digital assets, protect privacy, monitor and record interactions, and to know when interactions are compromised are the same. The same diligent practices must be followed and the capabilities in Hogg, Anderson, Shapiro, Rudolf and Cree meet the needs of any of the secure facilities. For example, Hogg discloses, that “[i]n many environments, monitoring of telephony calls to detect and/or prevent unauthorized activities is desirable,” (Ex. 1006,1:45-46) and cites to examples such as health care facilities and restricted living quarters such as military barracks. *Id.*, 4:66-5-9. And Shapiro also discloses that prisons are just an example of the restrained environments for its system. Ex. 1008, [0008]. And Rudolf discloses that its teachings can be used with any video communication system. Ex. 1009, [0050].

233. Indeed, the ‘292 Patent admits that its technology is applicable beyond prisons: “... the embodiments described herein could be used in any facility requiring consolidated secure services.” Ex. 1001, 2:43-45. As such, a POSITA would not to be limited to disclosures concerning prisons; but would look to disclosures concerning a broad range of secure environments, including government and military applications as disclosed by Anderson. In my experience, I would expect any POSITA to explore possibilities from any industry or experience to identify tools, technologies, processes, or configurations that would enhance the capabilities. For example, in my experience we focused a great deal on technologies provided for education and financial industries in addition to law enforcement and correctional environments.

234. A POSITA would also be motivated to combine the teachings of Hogg, Anderson, Shapiro, Rudolf, Swanson, Cree and Swink as each of these references provide various solutions for electronic communications and security in many environments. With access to each of these prior art patents, a POSITA would naturally recognize the synergy between the disclosures and realize the combinations would enhance the ability to provide effective and secure transactions, communications and networks. For example, a POSITA would be motivated to include the teachings of Hogg in such a combination because Hogg discloses, embodiments “generally to use of biometric identification during a call for detecting an anomaly occurring in the call, such as a change in the parties participating on the call.” Ex. 1006, 4:44-47. Detecting anomalies in secure communications (i.e., video visitations, video calls, etc.) would be an important capability for use in secure environments. In any secure environment, the ability to recognize anomalies is extremely important whether the process is digital or physical. With in-person transactions, staff are looking for the passing of contraband or inappropriate information. In telephone calls, staff are looking for changes in parties and exchange of inappropriate information. In a video environment, staff are looking for similar anomalies, and it would be expected that the technology would supplement the capabilities of human staff.

235. A POSITA would be motivated to include the teachings of Anderson in such a combination because Anderson discloses, “means of permitting display of information to authorized users, while detecting, limiting or preventing disclosure to others, is needed.” Ex. 1007, 2:4-6. Controlling display of secure communications to authorized users, would be important in such secure environments. Safety and security in a secure facility take on many forms. The need to protect the specific content of an interaction may have been obvious, but there are many other needs as well. For example, in a video interaction, the control

of the background environment is important to ensure the identities and descriptions of staff or other offenders isn't made known to outside parties, thus putting the background parties or their families at risk. In another instance, an offender may be reporting inappropriate activities of a staff member or other inmate. In those instances, the display of content must be protected to ensure the safety and continued interaction of the reporting party.

236. A POSITA would be further motivated to include the teachings of Shapiro in such a combination because Shapiro discloses the combination of “delivering and monitoring electronic letters to correction facility inmates while giving supervisory authorities the ability to screen the incoming mail” (Ex. 1008, [0007]) with “a computer-operated kiosk that may be used by individuals (e.g., inmates) in a restrained environment/restricted-access location (e.g., a prison) to browse through a catalog of available digital media or content...” Id., Abstract. Providing such multiple-use kiosks in secure facilities for inmates would be important for use in such secure environments. In secure facilities, space and funding are often constraints. In addition, a common goal is to reduce the number of points of risk exposure. The ability to use a single device to provide multiple services, then, is a constant desire. The same is true in the facility itself. Classrooms are often used for activities ranging from inoculation clinics, self-help groups, or even staff training.

237. A POSITA would be further motivated to include the teachings of Rudolf, as Rudolf describes that its invention “may be particularly advantageous for minimizing visitation overhead, training, etc. for the correctional officers of a facility.” Ex. 1009, [0049]. Minimizing visitation overhead and training for the facility would be important for use in such secure environments. Visitation is often limited by space and staffing. The unfortunate consequence is that the number of visitors or the time of interaction between an inmate and the visitor is limited. The

use of digital tools allows the same number of staff to support many more visitations and reduces the need for mandatory overtime or training to expand the visitation capacity.

238. A POSITA would also be motivated to refer to Swanson in such combinations as it discloses solutions for “managing communications during a videoconference,” such as the video conferences disclosed by Hogg, Anderson and Rudolf. Ex. 1010, 1:26-32. Further Swanson discloses technology to “monitor and control access to traffic between a User A-F and the network 10.” *Id.*, 4:22-27. As such, a POSITA would be motivated to understand how Swanson’s traffic monitoring technologies could be useful in combination with Hogg’s desire to monitor calling activities between prisoners and other parties. No matter what the service that is ultimately provided (video visitation, music purchase, educational download), the IT network provides the backbone that transports the digital information. Monitoring and managing that backbone is one of the critical capabilities of an IT organization, whether vendor provided or in-house. IT staff are looking for compromises (information security) and for capacity/performance issues. Lost or degraded service can lead to inmate complaints and lawsuits which are just as concerning as privacy and security breaches.

239. A POSITA would also be motivated to refer to Cree in such combinations as it discloses that “an advantage of present invention is that inmates in a prison facility can be notified of pending messages in an efficient and economical manner.” Ex. 1011, 2:64-66. As such, a POSITA would be motivated to look to Cree’s disclosure of efficient and economic prisoner messaging for use with Hogg’s video conferencing systems or with Shapiro’s kiosk-based inmate messaging systems. The existence of an electronic messaging or video conferencing solution is of little consequence if an offender doesn’t have a means to know when a call or message is scheduled for them. A POSITA would naturally

be looking to combine capabilities for managing the entire process to ensure safety, security, and to reduce the cost/effort of the process.

240. A POSITA would also be motivated to refer to Swink in such combinations as it discloses “[s]ystems, apparatuses, and methods that can facilitate securing an electronic device and associated information.” Ex. 1012, Abstract. As such, a POSITA would be motivated to look to Swink’s disclosure for methods means to secure the prisoners’ kiosks and associated information. Securing electronic devices has been a long-standing need in secure facilities. From radios and televisions, to newer tablets, computers, and other devices, institution executives expect a POSITA to identify all means reasonable and possible to secure the infrastructure.

241. A POSITA is a skilled and experienced artisan, one who would commonly look to multiple solutions, such as disclosed in Hogg, Anderson, Shapiro, Rudolf, Swanson, Cree and Swink to improve upon and/or modify secure facility communications systems and methods. A POSITA in this environment is constantly looking for and evaluating new technologies and processes to improve operations and security. Residents/inmates are constantly trying to exploit vulnerabilities in the systems, so the constant growth in IT capabilities and security is needed and expected.

242. A POSITA would have a reasonable expectation of success combining Hogg, Anderson, Shapiro, Rudolf, Swanson, Cree and Swink at least because each discloses similar and related technologies as discussed above in Section VIII and ¶¶231, 232 & 234. Because all of Hogg, Anderson, Shapiro, Rudolf, Swanson, Cree and Swink are dealing with technologies that are normal and useful in a secured facility setting, a POSITA would not only understand how the differing capabilities could be combined, but would also understand how to use the combination to achieve the desired outcomes of capability, security, and safety.

For these same reasons, any combination of these similar and related technologies would render predictable results.

243. The nature of computing devices has changed since inception. No longer are systems comprised of large single-purpose technologies. As of the priority date of the '292 Patent, the industry has moved to small, inexpensive devices that can be combined using IT network connections to collectively provide capabilities that are lower cost and easily scalable. Standard computers, mice, cameras, and other peripherals can be combined with hardened cases to place devices in secured facilities. In addition, standard IT networks can be configured with strong security standards and designs to protect both information and to provide the ability to monitor the digital information transiting the network. Standard IT servers can be used with specialized software to provide the capabilities, monitoring, billing, and processes that are necessary in the secured environment as well. Along these lines, Anderson, Hogg, Shapiro, Rudolf, Swanson, Cree and Swink disclose applications implemented using non-specialized (i.e., generic) computer systems and equipment. Hogg discloses that its solutions can essentially be "implemented via software executed by a processor." Ex. 1006, 15:62-67. Anderson discloses exemplary embodiments implemented on generic computer equipment of Fig. 1 or Fig. 2. Ex. 1007, 8:44 to 9:19 and Figs. 1 & 2. Further, Anderson discloses that its disclosure "can be applied to any device that is capable of displaying information under computer control..." *Id.*, 9:34-38. Shapiro discloses that its solutions can be implemented on a generic computing environment as shown in Fig. 1, in addition to other "well known computing systems." Ex. 1008, [0024] – [0025]. Rudolf discloses that its solutions can be implemented on "any number and/or configurations of communication stations. Ex. 1009, [0017]. Swanson discloses that its solutions can be implemented in generic computer system equipment and software. Ex. 1010, 2:27-52. Cree

discloses a generic “telecommunication system” that can use a world-wide public telephone network or integrated into an inmate telephone system. Ex. 1011, 1:66-2:30. Likewise, Swink discloses generic communication devices operating on generic communication networks. Ex. 1012, [0038]-[0039].

244. As such, because no specialized computer systems are required by any of Anderson, Hogg, Shapiro, Rudolf, Swanson, Cree or Swink, a POSITA as a skilled and experienced artisan would have a reasonable expectation of success implementing the various solutions disclosed in any of Hogg, Anderson, Shapiro, Rudolf, Swanson, Cree and Swink into a single system and method using non-specialized computer equipment. Correctional Administrators routinely expect a POSITA in this environment to identify cost-effective mechanisms to deliver digital services. That expectation drives the desire to combine standard equipment that can be easily configured, deployed, and managed without exceptional cost or skill. A POSITA would understand the need to minimize complexity, minimize the number of devices and expand security capabilities and consequently would focus on using known and available devices and equipment. For these same reasons, the disclosed combinations would render predictable results. Because the configurations use normal devices that are often used in secured facilities, it is very reasonable to expect results that fulfill the intended objectives.

XII. DECLARATION

245. I hereby declare under the penalty of perjury that the following is true and correct. All statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true. In understand that perjury and/or willful false statement and the like are punishable by fine or imprisonment, or both (18 U.S.C. §1001).

Declaration of Russell J. Nichols in support of petition for *inter partes* review of
U.S. Patent No. 9,030,292

Date: January ^{24.00}____, 2024

1/24/2024 | 11:44 PM EST

Respectfully submitted,

DocuSigned by:

F57287F3FC4C41E...

Russell J. Nichols

Certificate Of Completion

Envelope Id: A883A6C49D13459CAE2FB887569FC975

Status: Completed

Subject: Complete with DocuSign: 2024-01-24 Nichols Declaration ISO Petition for IPR of US9030292.pdf

Source Envelope:

Document Pages: 136

Signatures: 1

Envelope Originator:

Certificate Pages: 4

Initials: 0

Monica Cantu

AutoNav: Enabled

1375 E. 9th Street

Envelope Stamping: Disabled

Cleveland, OH 44114

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

mlcantu@bakerlaw.com

IP Address: 97.137.121.105

Record Tracking

Status: Original

Holder: Monica Cantu

Location: DocuSign

1/24/2024 4:46:53 PM

mlcantu@bakerlaw.com

Signer Events

Russell Nichols

russ@rnicholsconsulting.com

Security Level: Email, Account Authentication
(None)**Signature**

DocuSigned by:



F57267F3FC4C41E...

Signature Adoption: Drawn on Device

Using IP Address: 73.41.153.74

Timestamp

Sent: 1/24/2024 4:49:30 PM

Viewed: 1/24/2024 11:43:25 PM

Signed: 1/24/2024 11:44:10 PM

Electronic Record and Signature Disclosure:

Accepted: 1/24/2024 11:43:25 PM

ID: 62ed6de2-4d5a-46e8-9017-eb8ff28ceb00

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	1/24/2024 4:49:30 PM
Certified Delivered	Security Checked	1/24/2024 11:43:25 PM
Signing Complete	Security Checked	1/24/2024 11:44:10 PM
Completed	Security Checked	1/24/2024 11:44:10 PM
Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Baker Hostetler LLP (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Baker Hostetler LLP:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: maylward@bakerlaw.com

To advise Baker Hostetler LLP of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at maylward@bakerlaw.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Baker Hostetler LLP

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to maylward@bakerlaw.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Baker Hostetler LLP

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to maylward@bakerlaw.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Baker Hostetler LLP as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Baker Hostetler LLP during the course of your relationship with Baker Hostetler LLP.