IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *inter partes* review of:
U.S. Patent 7,529,357 to Rae et al.
Filed: Herewith
For: **Inmate Management and Call Processing Systems and Methods**

Atty. Docket: 3210.048IPR3

Declaration of Dr. Leonard J. Forys in Support of Petition for *Inter Partes* Review of U.S. Patent No. 7,529,357

Attn: Patent Trial and Appeal Board
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450
Commissioner:

I, Dr. Leonard J. Forys, declare as follows:

1. I have been retained on behalf of Global Tel*Link Corporation ("GTL") for the above-captioned *inter partes* review proceeding. I understand that this proceeding involves U.S. Patent No. 7,529,357 ("the '357 patent") titled "Inmate Management and Call Processing Systems and Methods" by Robert L. Rae, et al., and that the '357 patent is currently assigned to Securus Technologies, Inc. I understand that claims 1, 3, 4, 6, 7-13, 19 and 20 were found to be unpatentable in a prior *inter partes* review proceeding.

SKI Exhibit 2051

Page 1 of 101

2. I have reviewed and am familiar with the specification of the ’357 patent. I understand that the ’357 patent was filed on July 12, 2007 as a continuation-in-part of U.S. Patent No. 7,899,167 (“the ’167 patent”) filed on August 15, 2003. I understand that the Patent Owner represented that the remaining claims of the ’357 patent (claims 2, 5, 8, 9, 11, 12, and 14-18) are only entitled to claim priority to the July 12, 2007 filing date of the ’357 patent. While I disagree with the Patent Owner’s representation, I used July 12, 2007 as the priority date for the challenged claims in this proceeding

3. I have reviewed and am familiar with the file history of the ’357 patent. I understand that the file history has been provided as Exhibit GTL 1002. I have reviewed and am familiar with the file history of the prior *inter partes* review proceeding involving the ’357 patent (IPR2014-00825).

4. I have also reviewed and am familiar with the following prior art used or cited in the Petition for *inter partes* review, the Petition for covered business method review of the ’357 patent, the prior *inter partes* review of the ’357 patent, and the prior *inter partes* review of the ’167 patent:

> **SR-4717, Voice Over Packet in Next Generation Networks: An Architectural Framework** by Bellcore (“Bellcore”) published in January 1999, more than eight years prior to the filing date of the

’357 patent. I understand that Bellcore is provided as Exhibit GTL 1004.

U.S. Patent No. 7,333,798 to Hodge, titled “Telecommunication Call Management and Monitoring System,” (“Hodge”) published on February 12, 2004, over three years prior to the filing date of the ’357 patent. I understand that Hodge is provided as Exhibit GTL 1005.

U.S. Patent No. 6,831,556 to Boykin, titled “Composite Mobile Digital Information System,” (“Boykin”) issued on December 14, 2004, more than two years prior to the filing date of the ’357 patent. I understand that Boykin is provided as Exhibit GTL 1006.

U.S. Patent No. 5,861,810 to Nguyen, titled “System and Method for Providing Crime Victims Updated Information and Emergency Alert Notices,” (“Nguyen”) issued on January 19, 1999, more than eight years prior to the filing date of the ’357 patent. I understand that Nguyen is provided as Exhibit GTL 1007.

Criminal Calls: A Review of the Bureau of Prisons’ Management of Inmate Telephone Privileges (“Criminal Calls”) by the U.S. Department of Justice, Office of the Inspector General published in August 1999. I understand that Criminal Calls is provided as Exhibit GTL 1008.

U.S. Patent No. 4,054,756 to Comella, titled “Method and Apparatus for Automating Special Service Call Handling,” (“Comella”) issued on October 18, 1977. I understand that Comella is provided as Exhibit GTL 1010.

PacketCableTM 1.0 Architecture Framework Technical Report, PKT-TR-ARCH-V01-001201, by Cable Television Laboratories, Inc. published in 1999. I understand that PacketCable is provided as Exhibit GTL 1011.

Voice Over Internet Protocol (VoIP), Proceedings of the IEEE, Vol. 90, No. 9, 1495-1517 ("Goode") published in September 2002. I understand that Goode is provided as Exhibit GTL 1012.

U.S. Patent No. 7,899,167 to Rae, titled "Centralized Call Processing" ("Rae") issued on March 1, 2011. I understand that Rae is provided as Exhibit GTL 1013.

U.S. Patent No. 7,505,406 to Spadaro, titled "Public Telephone Control with Voice over Internet Protocol Transmission," ("Spadaro") was filed on July 13, 2001, almost six years prior to the filing date of the '357 patent. I understand that Spadaro is provided as Exhibit GTL 1014.

Science Dynamics, SciDyn BubbleLINK ("BubbleLink") archived June 18, 2006. I understand that BubbleLink is provided as Exhibit GTL 1017.

BOP Historical Timeline, accessed October 11, 2016. I understand that BOP Historical Timeline is provided as Exhibit GTL 1018.

SENTRY Audit Report No. 0325 ("SENTRY Audit Report") published in July 2003. I understand that SENTRY Audit Report is provided as Exhibit GTL 1019.

Privacy Impact Assessment for the SENTRY Inmate Management System ("SENTRY Impact Assessment") published in July 2012. I understand that the SENTRY Impact Assessment System is provided as Exhibit GTL 1020.

U.S. Patent No. 8.031,849 to Apple *et al.*, titled "Telephony System and Method with Enhanced Fraud Control," ("Apple") was filed on September 2, 2005, more than a year prior to the filing date of the '357 patent. I understand that Apple is provided as Exhibit GTL 2021.

Inmate Security Designation and Custody Classification Program Statement ("SENTRY Program Statement") published in September 2006. I understand that the SENTRY Program Statement is provided as Exhibit GTL 1022.

U.S. Patent No. 7,197,560 to Caslin, titled "Communications System with Fraud Monitoring" ("Caslin") issued on March 27, 2007. I understand that Caslin is provided as Exhibit GTL 1023.

SIP and IPLink and the Next Generation Network ("SIP and IPLink") published in 2001. I understand that SIP and IPLink is provided as Exhibit GTL 1024.

Commander II published March 6, 2002. I understand that Commander II is provided as Exhibit GTL 1025.

SR-2275, Bellcore Notes on the Networks ("Bellcore Notes") published December 1997. I understand that Bellcore Notes is provided as Exhibit GTL 1026.

Engineering and Operations in the Bell System ("Engineering and Operations") published in 1984. I understand that Engineering and Operations is provided as Exhibit GTL 1027.

U.S. Patent No. 4,191,860 to Weber, titled "Data Base Communication Call Processing Method" ("Weber") issued March 4, 1980. I understand that Weber is provided as Exhibit 1028.

A Telecommunications Buildings/Power Infrastructure In A New Era of Public Networking by Nicholas Osifchin (IEEE 2000). I understand that Osifchin is provided as Exhibit GTL 1029.

Murder Suspect Arrested, LAPD News Release, April 24, 2002 (LAPD News Release). I understand that the LAPD News Release is provided as Exhibit GTL 1032.

5. The '357 patent describes "systems and methods that provide centralized or nodal inmate management and telephone processing capabilities." ('357 patent, Abstract.) I am familiar with the technology described in the '357 patent as of its filing date of July 12, 2007 (alleged priority date of the remaining claims).

6. I have been asked to provide my technical review, analysis, insights, and opinions regarding the '357 patent and the references discussed in the *inter partes* review of the '357 patent.

I. Qualifications

7. I have nearly 50 years of experience in the telecommunications industry working for corporations including AT&T Bell Telephone Laboratories for almost two decades and Bellcore (formerly Bell Communications Research), the research and development organization for the Bell Operating Companies (*e.g.*, Bell Atlantic, Southwestern Bell, US West, etc.), for over a decade. As detailed below, I have worked on many projects and technologies highly relevant to the subject matter of the '357 patent.

8. My academic background in electrical engineering and computer science provides a technical foundation for work in telephone communications networks. I received a Bachelor of Science Degree in Electrical Engineering from the University of Notre Dame in 1963. I received both a Master of Science in Electrical Engineering and the degree of Electrical Engineer from the Massachusetts Institute of Technology in 1965. I received a degree of Doctor of Philosophy in Electrical Engineering and Computer Science from the University of California at Berkeley in 1968.

9. While at Berkeley, I was an Assistant Professor of Electrical Engineering and Computer Science, teaching courses in network theory, systems theory and communications theory, performing research in communications systems and serving as faculty advisor to 20 undergraduates.

10. From 1968 to 1973, I was a member of the technical staff at Bell Telephone Laboratories (known commonly as Bell Labs). I engaged in various research activities involving network engineering and performance management in telephone networks. I taught several in-house courses in performance analysis and traffic engineering in telephone networks.

11. From 1973 to 1984, I was a Technical Supervisor at Bell Telephone Laboratories, heading a group of technical experts, primarily Ph.D.'s. I was responsible for performance management/analysis and development of traffic engineering algorithms for various telecommunications networks and their components, primarily processor based voice switches, automatic call distributors, and Private Branch Exchanges ("PBXs"). As part of this effort, I successfully rescheduled the processor tasks in several of these systems to increase their capacity and improve their performance. I also was responsible for all of the call center staffing algorithms for the Bell System and for the engineering of the network elements used for call centers such as the TSPS (Traffic Service Position System), Rockwell ACDs, and the #5 CrossBar ACD. ACDs are Automatic Call Distributors, special purpose switches used to provide call center functionality. In particular, these network elements were used during this time period to provide collect calling for inmate phones as they handled both automatic and operator assisted coin phones and automatic and assisted collect calling. I note that these network elements were cen-

tralized, deployed remotely from the prison facilities and served multiple prison facilities.

12. From 1984 to 1994, I was a District Manager for Bell Communications Research ("Bellcore"), heading a group of 7 to 15 technical experts, primarily Ph.D.'s. I was responsible for the specification and testing of a variety of voice network components. This work included writing sections of the requirements used by the Bell Operating Companies to buy network components in their networks. I also tested the compliance (to the requirements) of several voice switches made by various companies (*e.g.*, Nortel, Lucent, Ericsson, Fujitsu, NET, and Siemens).

13. During this time period, I further consulted on the engineering and performance of various supplemental telephonic services such as Voice Mail systems, including those manufactured by Boston Technologies, Unisys, and Digital Sound Corporation, as well as supporting equipment such as SMDI (Simplified Message Display Interface) links. Thus, I am familiar with the types of recording technologies available to record inmate conversations prior to the alleged priority date of the remaining claims of the '357 patent. I also participated and contributed to various national and international voice and data standards organizations.

14. During this period, I continued my involvement with call center technology. In particular, I was responsible for the engineering of all call centers for

the Bell Operating Companies. This included analyzing specific network elements used to handle inmate telephone calls such as Nortel's TOPS (Traffic Operator Position System) and MPP (Multi-Purpose Position) systems and AT&T's No. 5 OSPS (Operator Services Position Station).

15. Another of my responsibilities while at Bellcore was analyzing and providing engineering algorithms for data network components used by the Bell Operating Companies. As part of this endeavor, I was a leader in developing novel traffic engineering methods for Internet data networks and other high speed data networks such as Asynchronous Transfer Mode (ATM) and Frame Relay. This included characterizing Internet traffic and developing loading guidelines for network components including routers and switches. Through this effort, I worked on some of the earliest deployed packet-based networks, some of which included voice over packet technologies.

16. I was Bellcore's prime technical leader for determining root causes of, and proposed solutions for, several Signaling System No. 7 ("SS7") data network outages, including the famous 1990 AT&T nationwide outage, as well as the 1991 Washington, D.C., Pittsburgh, and Los Angeles outages. I was responsible for writing new sets of requirements for SS7 networks and was involved in a large scale testing and analysis program for a wide variety of SS7 network components.

17. I was named a Bellcore Fellow in 1992, only the fifth person to receive such an award.

18. From 1994 to 1995, I was a Chief Scientist at Bellcore, overseeing the technical work of 50 technical experts, many of whom had Ph.D.'s. I was involved in the teaching of teletraffic engineering and performance management to various bodies, including the Federal Communications Commission, which included various aspects of both voice and data networks, including voice mail systems. I served as a "trouble shooter," responsible for identifying root causes for diverse network problems involving a variety of technologies including both high speed data networks as well as telephone networks. I analyzed the potential impact of earthquakes and other natural disasters on telecommunications network performance. The National Science Foundation sponsored me to be the sole U.S. telecommunications industry representative at the First International Joint U.S.-Japan Earthquake Symposium in 1993.

19. Since 1995, I have been President of my own company, The Forys Consulting Group, Inc., providing consulting in voice and data communications services. Relevant to the subject matter of this case, I used HP's SS7 network monitoring capabilities to analyze Internet traffic patterns in a large metro area. As part

of a team of international experts, I investigated a wide range of issues involving the introduction of a new line of vendor products in a foreign national network.

20. As a consultant to a large telephone company, I advised them on quality of service issues in providing voice over ATM (with and without IP), Internet and Multiprotocol Label Switching (MPLS) networks. I further analyzed various supplier components for providing hybrid fiber coax access in cable networks. I consulted with a large company on the economic and technical problems associated with providing voice and data communications over a foreign cable network.

21. During this period, I also performed extensive consulting for various data communications systems, including Internet access using satellite systems including LAN in the sky technologies for airplanes. I analyzed the performance, provided traffic inputs and helped specify traffic network management/congestion controls for three satellite data communications systems capable of handling both packetized voice as well as Internet traffic.

22. I experimented with some of the first VoIP systems, including a 1996 version of Vocaltec's Internet Phone.

23. My Curriculum Vitae is attached as Exhibit GTL 1003, which contains further details on my education, experience, publications, and other qualifications to render an expert option. My work on this case is being billed at a rate of $400.00

per hour, with reimbursement for actual expenses. My compensation is not contingent upon the outcome of this *inter partes* review.

II. My Understanding of Claim Construction

24. I understand that, during an *inter partes* review, claims are to be given their broadest reasonable construction in light of the specification as would be read by a person of ordinary skill in the relevant art.

25. I understand in the prior *inter partes* review proceeding the Board construed the term "*call application management system*" as a system that performs the enumerated function of "connecting a call to or from the telephone terminals over telephone carrier network responsive to receiving a request for connecting the call." (IPR2014-00825, Final Written Decision, p. 26.) For purposes of this proceeding, I adopt this construction.

III. My Understanding of Obviousness

26. I understand that a patent claim is invalid if the claimed invention would have been obvious to a person of ordinary skill in the field at the time the application was filed. This means that even if all of the requirements of the claim cannot be found in a single prior art reference that would anticipate the claim, the claim can still be invalid.

27. As part of this inquiry, I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- 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.

28. To obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of the prior art in the field. I understand that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art.

29. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to (1) identify the particular references that, singly or in combination, make the patent obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain how the prior art references could have been combined in order to create the inventions claimed in the asserted claim.

30. I understand that certain objective indicia can be important evidence regarding whether a patent is obvious or nonobvious. Such indicia include: commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention as compared to the closest prior art; praise of the invention by the infringer or others in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee proceeding contrary to the accepted wisdom of the prior art. I am not aware of any secondary considerations of non-obviousness regarding the '357 patent

IV. Level of Ordinary Skill in the Art

31. I understand the Board in the prior *inter partes* review proceeding determined that one of ordinary skill in the art would have a B.S. degree in Electrical Engineering, Computer Science, or an equivalent field as well as at least three years of academic or industry experience in telephony systems. (IPR2014-00825, Final Written Decision, p. 29.) The Board's construction is consistent with the level of ordinary skill that I proposed in the prior IPR proceeding. For purposes of this proceeding, I adopt the Board's level of ordinary skill in the art.

V. Overview of the ’357 patent

32. The ’357 patent describes “systems and methods that provide centralized or nodal inmate management and telephone call processing capabilities.” (’357 patent, Abstract.) Centralization of information management, according to the ’357 patent, provides the benefits of data sharing, aggregation, and analysis across multiple served facilities. (*See, e.g.,* ’357 patent, 3:65-4:6.)

33. I understand that the ’357 patent is a continuation-in-part of U.S. Patent No. 7,899,167. The claims of the ’167 patent are directed to the “telephone call processing capabilities” of the system. Independent claim 1 (reproduced below) includes a networking device, an unauthorized call activity detection system, a call application management system, and a billing system.

> 1. A centralized call processing system for providing call processing services to a plurality of prison facilities, comprising:
>
> a networking device connected via digital data links to call processing gateways at the plurality of prison facilities to collect outgoing Voice over Internet Protocol (VoIP) data packets associated with calls from the plurality of prison facilities and to distribute incoming VoIP data packets associated with the calls to the plurality of prison facilities, the plurality of prison facilities located remotely from the call processing gateways, each of the plurality of prison facilities including at least one telephone terminal;

an unauthorized call activity detection system co-located with the networking device and connected to the networking device for detecting three-way call activity associated with the calls placed from one or more of the plurality of telephone terminals, the three-way call activity detection not performed at the plurality of the prison facilities;

a call application management system co-located with the networking device and connected to the networking device and the unauthorized call activity detection system for at least processing the outgoing VoIP data packets from the plurality of prison facilities into outgoing call signals and transmitting the outgoing call signals to a first telephone carrier network, the call application management system receiving incoming call signals from the first telephone carrier network and processing the incoming call signals into the incoming VoIP data packets for distribution to the plurality of prison facilities by the networking device; and

a billing system co-located with said call application management system and located remotely from the call processing gateways, the billing system connected to the call application management system for providing accounting of the calls.

34. I understand that the Board found all claims of the '167 patent unpatentable over the applied art. (IPR2014-00493, Final Written Decision.) I further understand that the Federal Circuit affirmed the Board's findings. *Securus*

Technologies, Inc. v. Global Tel Link Corporation, Appeal No. 2016-1372, 2016-1373, Fed. Cir. R. 36 Affirmance (Dec. 8, 2016).

35. I further understand that claims 1, 3, 4, 6, 7, 10, 13, 19, and 20 of the '357 patent were found unpatentable over the applied prior art in the prior *inter partes* review proceeding. Independent claim 1 of the '357 patent (reproduced below) has two call processing limitations, "networking device" and the "call application management system," and a single date storage/management system component: "inmate management system." These claims merely add the component of centralized data storage and management to portions of the telephone call processing capabilities recited in the '167 patent and found unpatentable by the Board in the '167 IPR proceeding. The '357 patent does not add or purport to add any new call processing capabilities. The recited information management, networking, and call processing components recited in claim 1 of the '357 patent are conventional and operate for their usual and intended purpose.

> 1. A computer-based system, at a plurality of facilities, for managing inmate information, each of the facilities having one or more telephone terminals and computer terminals, the computer-based system located remotely from at least one of the plurality of facilities, the system comprising:
>
> a networking device exchanging Voice over Internet Protocol (VoIP) data packets with call processing gateways at the plural-

> ity of facilities over digital data links, the call processing gateways processing the VoIP data packets to or from the telephone terminals for transmission over the digital data links;
>
> an inmate management-system coupled to the networking device for providing shared data access of inmate records to computer terminals at said plurality of facilities, said inmate records created with first inmate information collected from a first computer terminal at a first facility of the plurality of facilities and modified responsive to collecting second inmate information from a second computer terminal at a second facility of the plurality of facilities; and
>
> a call application management system connecting a call to or from the telephone terminals over a telephone carrier network responsive to receiving a request for connecting the call and the call being authorized based on the inmate records provided by the inmate management system.

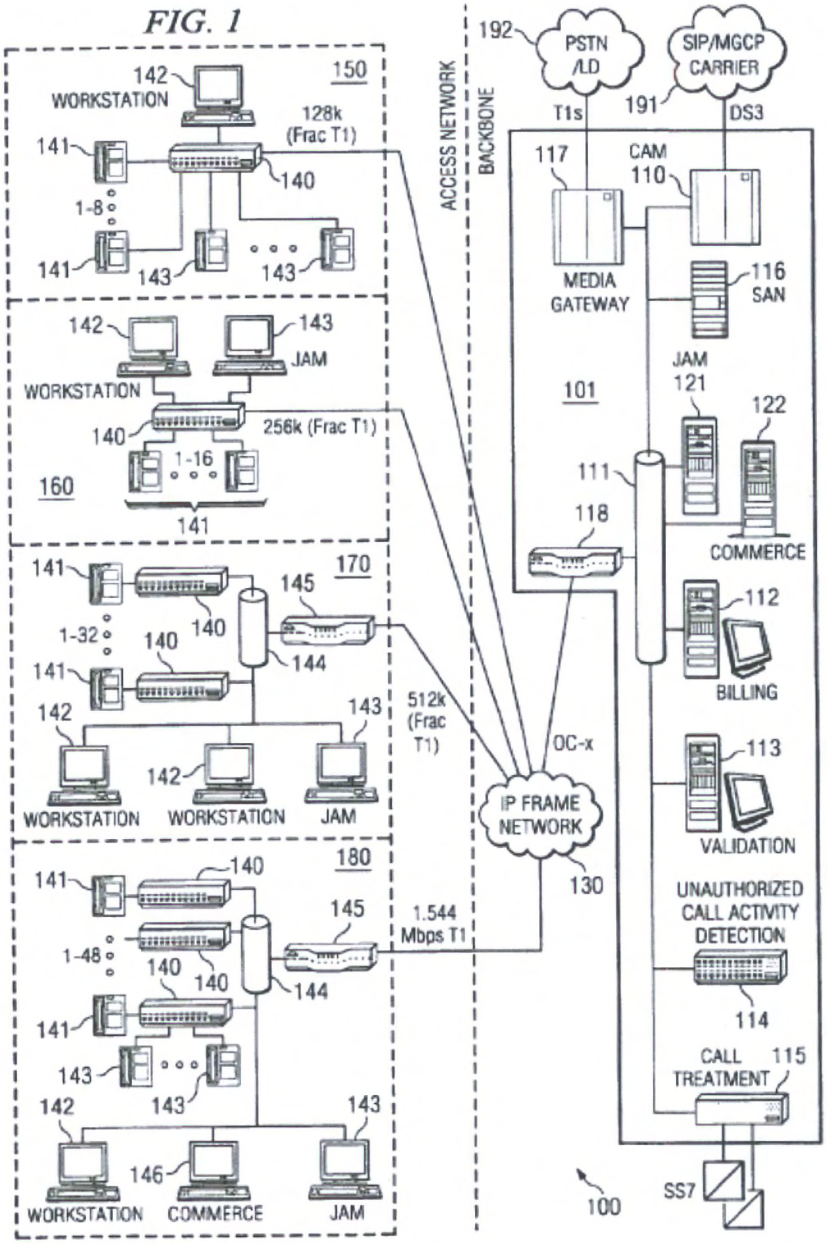
Independent claim 10 is a method claim corresponding to system claim 1. Claim 10 recites the same conventional actions performed by the conventional components of claim 1.

36. As I detail below, the centralized storage and management of data (including inmate data) was not only known but it was conventional before the July 12, 2007 filing date of the '357 patent. For example, the Federal BOP used a centralized system (SENTRY) to store and manage inmate data as early as 1978, as I discuss in further detail below. (*See, e.g.,* Exh. 1019, SENTRY Audit Report;

SENTRY Program Statement.) Thus, the '357 patent claims conventional inmate management and permits access to the centralized inmate management system from multiple remote facilities. Further, the ability for a first terminal to create a record in a centralized database and a second terminal at a different location to modify that record was standard and in-use in database systems prior to the July 12, 2007 filing date of the '357 patent. The SENTRY system is designed to provide exactly this functionality. The Board recognized that claims 1, 3, 4, 6, 7, 10, 13, 19, and 20 were obvious over the applied Spadaro and Hodge grounds in the prior IPR proceeding. The remaining dependent claims merely use the conventional technology recited in independent claims 1 and 10 and the claims of the '167 patent in well-known and routine ways.

37. Figure 1 of the '357 patent (reproduced below) illustrates "an inmate management and call processing system according to an embodiment of the present invention." ('357 patent, 6:25-26.) The call processing system 100 includes a "computer-based platform 101 in communication with facilities 150-180 via network 130." ('357 patent, 6:40-42.)

FIG. 1



38. As illustrated in Figure 1, one or more call processing gateways 140 are disposed "at or near sites for which inmate management and call processing services are to be provided, here facilities 150-180." ('357 patent, 6:67-7:3.) The call processing gateways 140 "provide interfacing and arbitration between a number of

protocols, signals, and/or interfaces." ('357 patent, 7:3-5.) The '357 patent acknowledges that the use of VoIP, including call processing gateways that convert calls to and from VoIP, existed in the prior art: "Embodiments of the present invention utilize commercially available devices, such as the IAD 2400 series of integrated access devices available from Cisco Systems, Inc., San Jose, Calif., in providing a call processor gateway." ('357 patent, 7:20-23.)

39. Computer-based platform 101 "includes router-switch 118 coupling network 130 to various systems and components comprising computer-based platform via network 111." ('357 patent, 8:41-44.) The claims refer to router/switch 118 as a "networking device [that] exchang[es] Voice Over Internet Protocol (VoIP) data packets with call processing gateways." Routers and switches capable of exchanging VoIP traffic with other components were known and in common use before July 12, 2007. For example, Bellcore discloses a core network that uses routers (Exh. 1026, Bellcore, p. 5-56); and both PacketCable and Goode disclose the use of routers for VoIP network traffic. (Exh. 1011, PacketCable, p. 10; Exh. 1012, Goode, p. 2.) Exchanging IP packets (including VoIP packets) is a conventional function of a router/switch. Thus, the '357 patent uses its "networking device" (router/switch) for its ordinary purpose. Computer-based platform 101 also includes multiple functional components: a call application management system

110, a billing system 112, a validation system 113, an unauthorized call activity detection system 114, and a call recording system.

VI. Background of the Technologies Disclosed in the '357 patent

A. Voice over IP Networks

40. The first commercial VoIP product was introduced by VocalTec Communications Ltd. in 1995. Over the next eight years, VoIP implementations by telecommunications carriers increased dramatically. In 1999, industry experts estimated that approximately 10% of all voice traffic would be carried over a VoIP network by 2003. (Bellcore, 1-1.) By the July 12, 2007 filing date of the '357 patent, the use of VoIP for voice communications was well-established and routine.

41. The underlying VoIP architecture disclosed and claimed in the '357 patent was well-known prior to the filing date of the '357 patent (July 12, 2007). This VoIP architecture was used by local exchange carriers (*e.g.*, Verizon), interexchange carriers (*e.g.*, MCI and Level 3), and even cable providers (*e.g.*, Cox) before 2007. For example, SR-4717, Voice over Packet in Next Generation Networks: An Architecture Framework by Bellcore, published over eight years before the '357 patent, describes VoIP networks used by carriers. U.S. Patent No. 7,197,560 to Caslin, *et al*, filed more than five years and published before the filing date of the '357 patent, depicts a VoIP architecture utilized by an interexchange carrier. "PacketCable 1.0 Architecture Framework Technical Report" published in

1999 (more than seven years before the filing date of the ’357 patent) depicts a VoIP architecture utilized by cable providers. “SIP and IPLink in the Network Generation Network” by Intel published in 2001 also discloses a VoIP architecture.

42. Additionally, during the *inter partes* review of the parent patent of the ’357 patent, U.S. Patent No. 7,899,167, the Patent Owner submitted exhibits that depicted VoIP architectures in existence before the filing date of the ’357 patent. For example, “Voice Over Internet Protocol (VoIP)” by Bur Goode published in September 2002 describes VoIP architectures including an architecture in which end user customers (*e.g.*, businesses), have local gateways to access an IP network. (Exh. 1012, Goode, p. 2, Figure 1.) Additionally, the Science Dynamics documents including BubbleLink document architecture and the Commander II document, illustrate that VoIP products were used in prison environments prior to the July 12, 2007 filing date of the ’357 patent. (*See, e.g.,* Exh. 1017, BubbleLink; Exh. 1025, Commander II.)

B. Centralization

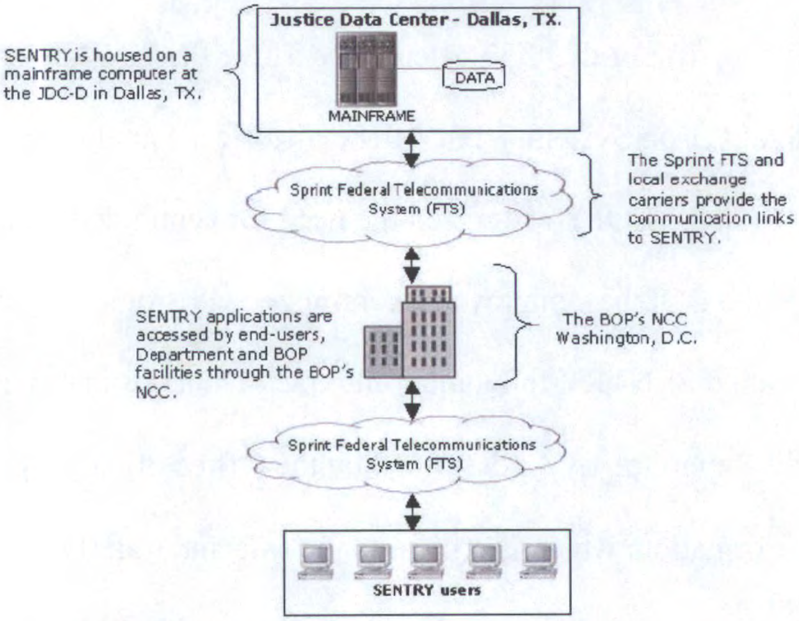
43. The ’357 patent describes “systems and methods that provide centralized or nodal inmate management and telephone call processing.” (’357 patent, Abstract.) In this architecture, certain call processing functions are centralized (located remotely from facilities). The “Background of the Invention” section of the ’357 patent sets out a list of motivations for moving from a distributed architecture

in which functionality is implemented locally at each location where service is provided to a centralized architecture in which a single piece of equipment serves multiple locations. These motivations include simplifying maintenance ('357 patent, 5:44-64); and increasing data sharing, aggregation, and statistical analysis. ('357 patent, 3:65-4:6.) In addition, the '167 patent (to which the '357 claims priority) also touts the benefits of reducing the cost and complexity of introducing new features. ('167 patent, 2:46-52.) As explained below, these are the same motivations that drove telecommunications carriers to centralized architectures for call processing and information management decades before the alleged priority date of the remaining claims of the '357 patent.

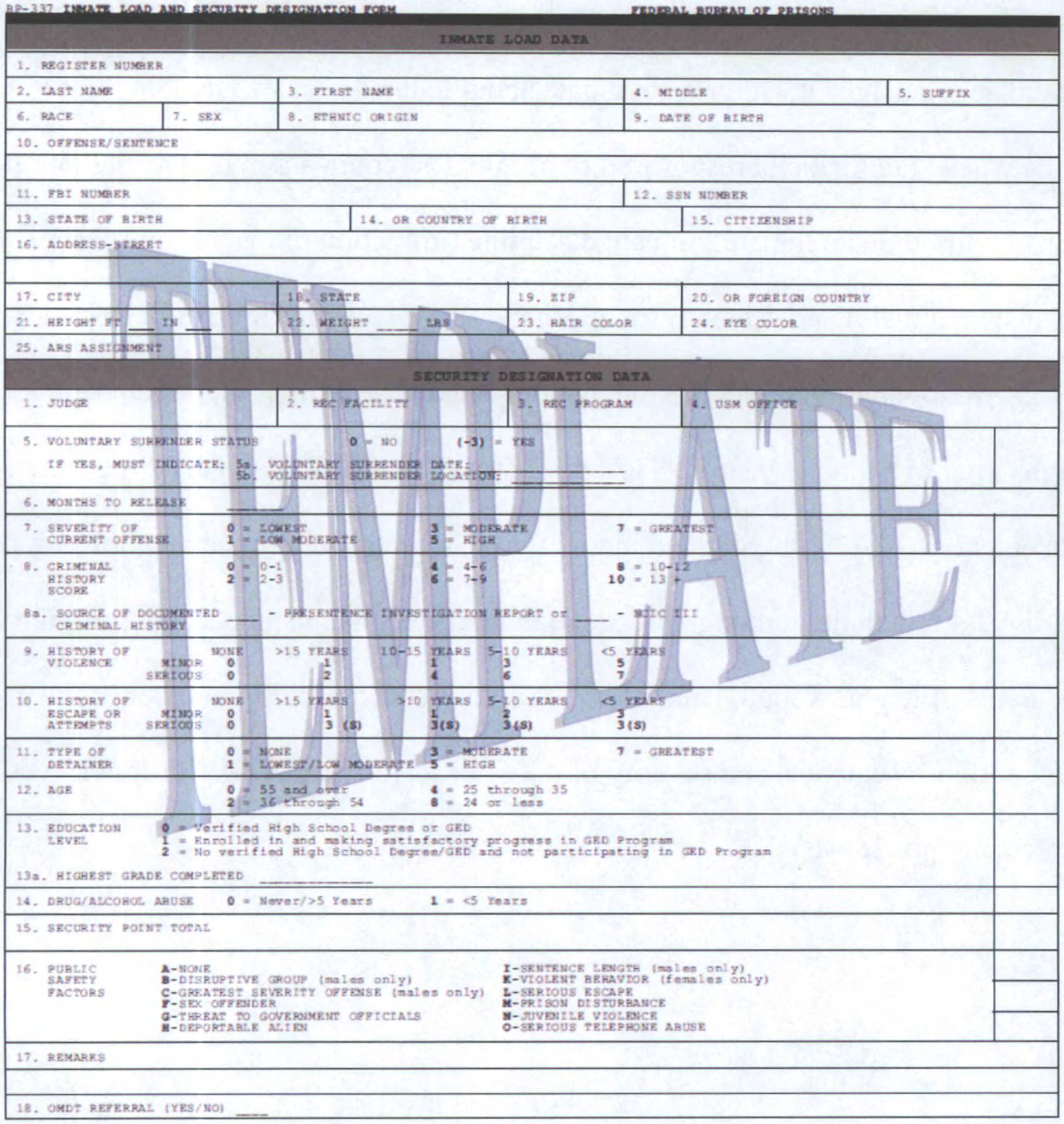
44. Centralization of inmate management was also routine decades before the July 2007 filing date of the '357 patent. The Three Prisons Act in 1891 established the Federal Prison System. (Exh. 1018, Historical Timeline, p. 1.) The Federal Bureau of Prisons (BOP) recognized the need for centralization of inmate data and since 1978, the BOP has employed a centralized electronic "inmate management system" called SENTRY to monitor and track federal inmates. (Exh. 1019, SENTRY Audit Report, p. 1.) As described by the Office of the Inspector General, "[a]ll inmate information, which is critical to the safe and orderly operation of BOP facilities, is collected, maintained, and reported within SENTRY." (SENTRY Audit Report, p. 1.) The following Figure (reproduced from the SENTRY Audit

Report) depicts the centralized management of inmate information. SENTRY "resides on a BOP mainframe computer located at the Justice Data Center in Dallas, Texas (JDC-D) operated by the Department of Justice (Department) Justice Management Division's (JMD) Computer Services." (*Id.*, p. 2.) Personal computers "at approximately 200 facilities in the Department and BOP" access SENTRY "by way of the BOP's Washington, D.C., Network Control Center." (*Id.*) "The remote sites include federal correctional facilities, regional offices, Community Corrections Offices (CCO), and other selected offices." (*Id.*, p. 2.) Through this centralized architecture, "SENTRY allows concurrent sharing of data among multiple users." (*Id.*, p. 3.)

SENTRY Network Configuration


Justice Data Center - Dallas, TX.
SENTRY is housed on a mainframe computer at the JDC-D in Dallas, TX.
DATA
MAINFRAME
Sprint Federal Telecommunications System (FTS)
The Sprint FTS and local exchange carriers provide the communication links to SENTRY.
SENTRY applications are accessed by end-users, Department and BOP facilities through the BOP's NCC.
The BOP's NCC Washington, D.C.
Sprint Federal Telecommunications System (FTS)
SENTRY users

45. Prior to the 2007 filing date of the '357 patent, SENTRY centrally stored and managed a wide-range of data about federal inmates including general inmate data, the financial responsibility of inmates (court-ordered financial obligations imposed on an inmate), inmate discipline (infraction of institution rules filed against an inmate) and sentence monitoring. (*See*, *e.g.,* SENTRY Audit Report, p. 2.) The following figure depicts the inmate load and security designation data forms used to populate the SENTRY database. (Exh. 1022, SENTRY Program Statement, p. 41.) As highlighted in this figure, a centralized inmate record stored in SENTRY includes, among other data, the inmate's name, physical description of the inmate (height, weight, hair color, eye color), social security number of the inmate, offense/sentence, and severity of the offense. (*See,* SENTRY Program Statement, pp. 26-41.)



BP-337 INMATE LOAD AND SECURITY DESIGNATION FORM

FEDERAL BUREAU OF PRISONS

TEMPLATE

INMATE LOAD DATA

1. REGISTER NUMBER

2. LAST NAME | 3. FIRST NAME | 4. MIDDLE | 5. SUFFIX

6. RACE | 7. SEX | 8. ETHNIC ORIGIN | 9. DATE OF BIRTH

10. OFFENSE/SENTENCE

11. FBI NUMBER | 12. SSN NUMBER

13. STATE OF BIRTH | 14. OR COUNTRY OF BIRTH | 15. CITIZENSHIP

16. ADDRESS-STREET

17. CITY | 18. STATE | 19. ZIP | 20. OR FOREIGN COUNTRY

21. HEIGHT FT ___ IN ___ | 22. WEIGHT _____ LBS | 23. HAIR COLOR | 24. EYE COLOR

25. ARS ASSIGNMENT

SECURITY DESIGNATION DATA

1. JUDGE | 2. REC FACILITY | 3. REC PROGRAM | 4. USM OFFICE

5. VOLUNTARY SURRENDER STATUS **0** = NO **(-3)** = YES

IF YES, MUST INDICATE: 5a. VOLUNTARY SURRENDER DATE: ______________
5b. VOLUNTARY SURRENDER LOCATION: ______________

6. MONTHS TO RELEASE ______

7. SEVERITY OF CURRENT OFFENSE

0 = LOWEST	**3** = MODERATE	**7** = GREATEST
1 = LOW MODERATE	**5** = HIGH	

8. CRIMINAL HISTORY SCORE

0 = 0-1	**4** = 4-6	**8** = 10-12
2 = 2-3	**6** = 7-9	**10** = 13 +

8a. SOURCE OF DOCUMENTED CRIMINAL HISTORY ____ - PRESENTENCE INVESTIGATION REPORT or ____ - NCIC III

9. HISTORY OF VIOLENCE

	NONE	>15 YEARS	10-15 YEARS	5-10 YEARS	<5 YEARS
MINOR	0	1	1	3	5
SERIOUS	0	2	4	6	7

10. HISTORY OF ESCAPE OR ATTEMPTS

	NONE	>15 YEARS	>10 YEARS	5-10 YEARS	<5 YEARS
MINOR	0	1	1	2	3
SERIOUS	0	3 (S)	3(S)	3(S)	3(S)

11. TYPE OF DETAINER

0 = NONE	**3** = MODERATE	**7** = GREATEST
1 = LOWEST/LOW MODERATE	**5** = HIGH	

12. AGE

0 = 55 and over	**4** = 25 through 35
2 = 36 through 54	**8** = 24 or less

13. EDUCATION LEVEL
0 = Verified High School Degree or GED
1 = Enrolled in and making satisfactory progress in GED Program
2 = No verified High School Degree/GED and not participating in GED Program

13a. HIGHEST GRADE COMPLETED ____________

14. DRUG/ALCOHOL ABUSE **0** = Never/>5 Years **1** = <5 Years

15. SECURITY POINT TOTAL

16. PUBLIC SAFETY FACTORS

A-NONE
B-DISRUPTIVE GROUP (males only)
C-GREATEST SEVERITY OFFENSE (males only)
F-SEX OFFENDER
G-THREAT TO GOVERNMENT OFFICIALS
H-DEPORTABLE ALIEN
I-SENTENCE LENGTH (males only)
K-VIOLENT BEHAVIOR (females only)
L-SERIOUS ESCAPE
M-PRISON DISTURBANCE
N-JUVENILE VIOLENCE
O-SERIOUS TELEPHONE ABUSE

17. REMARKS

18. OMDT REFERRAL (YES/NO) ___

Maintenance

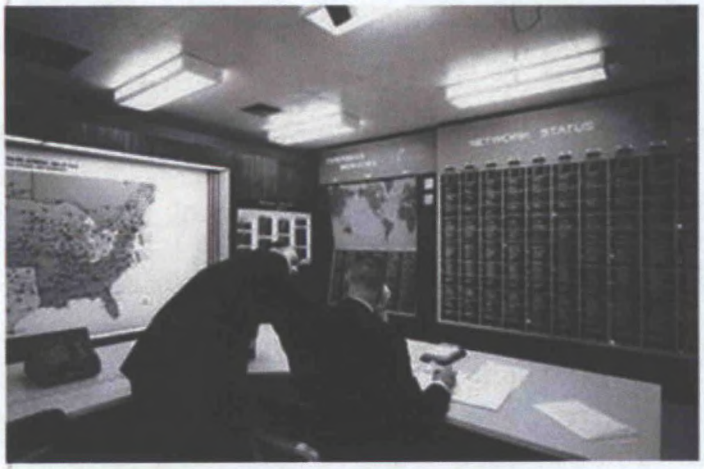
46. According to the ’167 patent, maintenance is generally viewed as encompassing “operations, administration, maintenance, and provisioning (OAM&P)” functions. (’167 patent, 2:12-34.) These OAM&P functions are typically performed by systems referred to as Operations Support Systems (OSSs).

47. By 1997, “[t]he maintenance plans for most Local Exchange Carrier (LEC) networks ha[d] evolved to a **centralized** method of operational and administrative control.” (Exh. 1026, Notes on Networks, 8-1 (emphasis added).) In fact, as noted in the 1997 Bellcore Notes on Networks, “[c]entralized databases and work forces make it possible to effectively maintain the precision and stability required for the current public switched network.” (Notes on Networks, 8-1.)

48. In the PSTN, these centralized databases and OSSs are known by their acronyms: CAROT (Centralized Automatic Reporting on Trunks), CATLAS (Centralized Automatic Trouble Locating and Analysis System), TIRKS (Trunks Integrated Network Keeping System), TNDS (Total Network Data System), EADAS (Engineering and Administration Data Acquisition System), etc. The CAROT, CATLAS, TIRKS, TDNS and EADAS systems existed and were in use at least two decades before the alleged priority date of the remaining claims of the ’357 patent. (Exh. 1027, Engineering and Operations in the Bell System, pp. 605-11, 622-

32, 638 and 650) Many of these systems are enormous. For example, TIRKS is a centralized system that supports the provisioning of many components of the PSTN. It is so large that it was rumored to require (at one point) 500 technical staff just to maintain it.

49. Another aspect of maintenance is network surveillance and monitoring. Systems for telecommunications network surveillance and monitoring have been centralized for more than four decades. For example, as early as 1962, the AT&T long distance network was centrally monitored from a Network Control Center in New York as depicted in the following photograph. (*See, e.g.,* http://www.corp.att.com/history.)[1]



AT&T Network Control Center, New York, 1960s.

[1] Pages from www.corp.att.com/history are provided as Exhibit GTL 1026.

50. In the 1970s, AT&T moved to a Network Operations Center (NOC) having domestic and international status boards, which automatically updated every 12 seconds, and computer databases to instantly provide managers with the information needed to reroute calls. By 1987, the centralized AT&T NOC had "a 75-screen video wall where computer-driven support systems provided information on multiple layers and categories of network activity. Managers used computer systems and terminals to find detailed information on any switch or route in the network. They then used those same systems to issue instructions to any place in the network." A picture of the AT&T NOC in 1987 is provided below. (*See, e.g.*, http://www.corp.att.com/history.)

1970s: Network Operations Center

AT&T Network Operations Center, Bedminster, N.J., 1987.

DATA SHARING, AGGREGATION, AND STATISTICAL ANALYSIS

51. The centralization of data was routine in telecommunications networks prior to the filing date of the '357 patent. One example of centralization of data is the Line Information Database (LIDB). LIDB stores data associated with customer

accounts, identified by individual line (*e.g.*, telephone numbers). (*See* Notes on Network, pp. 14-29.) LIDB stores the billing options for a line number/account including collect, calling card, and bill-to-third options for the account. (*Id.*) For certain types of billing options such as calling card, LIDB stores a PIN number for the account. (*Id.*, pp. 14-38.) LIDB also stores non-billing information about the line/number account. (*Id.*, pp. 14-29.) This non-billing information can include (*e.g.*, zip code) customer name or any other data element required by a network service. (*Id.*, pp. 14-29 to 30.)

52. The centralized OSSs and network operation centers described above aggregated data created and/or edited from terminals provided at multiple locations at a single network point. For example, the LIDB administrative system (AS/LIDB) is an OSS that maintains the data in LIDB. (*Id.*, pp. 14-29.)

Reducing the Cost and Complexity of Introducing Features

53. The centralization of call processing functionality to reduce the cost of services (deployment and maintenance) and to facilitate the introduction of new features and functions was also well-known in the telecommunications industry prior to the alleged priority date of the remaining claims of the '357 patent. For example, centralized switches that connected calls from telephones served by the switch to a carrier network were conventional and in user for more than 70 years.

Key examples of centralization of call processing functionality also include toll free (800) services and the advanced intelligent network (AIN).

54. Toll-Free (800) service was first introduced in 1967. (Notes on Networks, 14-41.) At that time, toll-free calls "were handled by designated originating and terminating switching offices that employed a special 800 NXX routing and screening methodology." (Notes on Networks, 14-41.) That is, calls to toll-free numbers were routed using a table at each central office switch. This distributed architecture required any updates, such as the addition of a new toll-free number, to be distributed to each of these multiple offices. As toll-free service grew in popularity, maintaining this distributed architecture became untenable. Therefore, in 1981, AT&T centralized 800 service using a centralized "database containing Toll-Free Service information" to determine the routing for the dialed toll-free number. (Notes on Networks, 14-41.)[2]

55. The Advanced Intelligent Network (AIN) "is an outgrowth of the architectures that were deployed for the intelligent network 800 Database Service and Alternate Billing Service (ABS)." (Notes on Networks, 14-58.) Prior to AIN, call

[2] Centralized 800 call handling is further described in U.S. Patent No. 4,191,860 to Weber, filed July 13, 1978. Weber is provided as Exhibit GTL 1028.

processing functionality was distributed in each switch. As explained in Notes on the Networks, the "basic concept of AIN is to migrate some service control functions from the switch to a LEC-programmable system so new services can be created rapidly and independently of the traditional switch vendor generic release cycles." (Notes on Networks, 14-58.) That is, the call processing functionality is deployed in a centralized system, referred to as the Service Control Point (SCP). Through AIN, new features and updates to existing features can be made at a centralized point in the network rather than in each switch.

C. Creating and Updating Records Using Different Terminals

56. With the advent of the Internet and other data networks, it was (and remains) commonplace to access, create and/or modify records in a centralized database from a multiplicity of terminals at various locations. For example, prior to the filing date of the'357 patent, users could modify their bank account information using a computer at work and alternatively a computer at home, or even a laptop while travelling. The availability of terminal facilities at airports, hotels, libraries, prisons etc. allowed records to be modified without owning a computer. ATM machines allowed customers to update records as well, withdraw money from one machine, deposit money at another, pay credit card bills, transfer money between accounts, etc.

57. Further, as I discussed above, the Federal BOP recognized the need to centralize data and allow for the creation and updating of records using different terminals at different facilities. The centralized SENTRY database "resides on a BOP mainframe computer located at the Justice Data Center in Dallas, Texas (JDC-D) operated by the Department of Justice (Department) Justice Management Division's (JMD) Computer Services." (SENTRY Audit Report, p. 2.) Personal computers "at approximately 200 facilities in the Department and BOP" access SENTRY "by way of the BOP's Washington, D.C., Network Control Center." (*Id.*) One of ordinary skill in the art would understand that it was not only obvious, but routine, prior to 2007 filing date of the '357 patent to use multiple terminals at different facilities to both create and update records stored in databases including inmate records.

D. History of Prison Communications

58. Inmate communications systems also followed the industry trend of centralization. As I described above, the Federal BOP implemented centralized storage and management of inmate data via its SENTRY system in 1978. The centralization of call processing followed this trend. The use of telephones by prison inmates was nearly non-existent up until the early 1970s. (Exh. 1008, USDOJ/OIG Special Report, 2.2.2.) Federal inmates were limited to one collect call every three months using staff telephones and this had to be reserved upon written request.

(USDOJ/OIG Special Report, 2.2.2.) In the 1970s, payphones were installed throughout most of the federal prison system, with no restrictions on the number of calls that could be made. (USDOJ/OIG Special Report, 2.2.2.)

59. Collect calls and coin phones, including collect calls from prison facilities, were normally handled by operator services switches managed by a carrier such as AT&T. These operator services switches were centralized in the carrier network and handled calls from multiple remote prison facilities. For example, U.S. Patent No. 4,054,756 to Comella (Exh. 1010), issued in 1977, introduced a centralized call processing facility for handling collect calls. Using Automatic Number Identification (ANIs), the operator services switches, such as the switches described in Comella, would access a database to determine, for example, that the origination was from a coin phone at a prison. Using this information, the switch and operators who handled the collect calls would be aware of any restrictions that might be made on such prison-originated calls.

60. By the late 1980s, there was a movement away from only using collect calls at prison facilities. Because of this trend, functionality for processing inmate calls was distributed to systems within individual prison facilities. For example, an Inmate Telephone System (ITS) was developed for the Federal Bureau of Prisons (BOP) in 1988. The ITS system consisted of computer hardware and software pro-

grams that enabled the BOP to debit inmates' commissary accounts for the cost of their calls. ITS used a computer, a telephone switch, and software that could control and record data regarding calls placed on telephones. Under ITS, each inmate received a "phone access code" (PAC), much like the calling card PIN, to facilitate this debiting and to (at least theoretically) permit correctional staff to identify which inmate made each call without visually checking the telephone area.

61. With the widespread deployment of VoIP in the late 1990s and early 2000s, inmate communications systems began to implement centralized call processing using VoIP technology. For example, U.S. Patent No. 7,505,406 to Spadaro (Exh. 1014) (filed over eight years before the '357 patent by Science Dynamics) applied the well-known centralization concept to inmate communications systems utilizing VoIP networks long before the filing date of the '357 patent. The documents cited by Patent Owner during the '167 patent IPR proceedings indicate that Science Dynamics also sold VoIP products targeted to prison facilities prior to the July 12, 2007 filing date of the '357 patent. I note that the Board found all claims of the '167 patent and the independent claims 1 and 10 and dependent claims 3, 4, 6, 7, 13, 19, and 20 of the '357 patent unpatentable over the applied Spadaro and Hodge grounds.

62. As I explained above, centralization of data management (including inmate management) and centralization of call processing was routine prior to the filing data of the ’357 patent. The prior art discussed above teaches that inmate management systems and call processing systems were conventional and well-known technology during the relevant timeframe. Below, when discussing the remaining claims of the ’357 patent, I highlight that the ’357 patent uses these existing systems in routine and logical ways to organize the activities and affairs of inmates, the way people in the federal prison system have done for generations. Indeed, the ’357 patent assumes that the recited information management, networking, and call processing components must operate in a conventional way. (*See, e.g.*, ’357 patent, 25:33-35, 7:12-16, 7:20-23, 9:10-14, 11:57-60.) The ’357 patent does not describe or claim any modification to the conventional operation of inmate management or call processing systems. The claims only require that the functions and steps be performed using generic computer-based systems, conventional telephones, and off-the-shelf networking equipment.

VII. Bellcore was Publicly Available Prior to the Filing Date of the ’357 patent

63. As discussed above, I held various positions at Bellcore (formerly Bell Communications Research) between 1984 and 1995. During that time, I became familiar with the publications produced by Bellcore, including Special Reports.

SR-4717, Voice Over Packet in Next Generation Networks: An Architectural Framework by Bellcore ("Bellcore") is a Special Report that was published by Bellcore in 1999 shortly after I left. The Bellcore reference was specifically published "to inform the industry of Bellcore's Voice Over Packet (VOP) Initiative." (Bellcore, p. iii.)

64. I have reviewed Exhibit GTL 1004 (which is a copy of Bellcore SR-4717), and based on my 11 years of experience at Bellcore, I believe Exhibit GTL 1004 to be a true and correct copy of Special Report-4717, "Voice Over Packet in Next Generation Networks: An Architectural Framework," by Bellcore. My opinion is based on the fact that Exhibit GTL 1004 is in a condition that creates no suspicion about its authenticity. Specifically, Exhibit GTL 1004 is not missing any intermediate pages, the text on each page appears to flow seamlessly from one page to the next, and there are no visible alterations to the document.

65. Moreover, based on my extensive experience at Bellcore, it is my opinion that the Bellcore reference would have been published and publicly available in or around January 1999. Indeed, the publication date of the Bellcore reference (January 1999) is clearly shown in the header of each page of the report. The header also indicates that the Bellcore reference is "Issue 1" of Special Report 4717, which further informs my opinion that the Bellcore reference would have been

published in January 1999. Furthermore, in my 11 years of experience at Bellcore, it was standard practice to make Special Reports (such as the Bellcore reference) publicly available in the month indicated in the header (*i.e.*, January 1999).

66. It is also my opinion that, by the end of January 1999, the Bellcore reference would have been sufficiently accessible to the public interested in the art, and an ordinarily skilled researcher, exercising reasonable diligence, would have had no difficulty finding a copy of the Bellcore reference. In fact, an ordinarily skilled researcher could have obtained a copy of the Bellcore reference in or around January 1999 by various means, including: (i) ordering the reference from Bellcore online catalog (telecom-info.bellcore.com); or (ii) contacting Bellcore Customer Service (mail, phone, or fax).

67. Therefore, it is my opinion that Exhibit GTL 1004 is an authentic document, and was publicly available well before the filing date of the '357 patent.

VIII. Bellcore in view of Hodge

68. Bellcore provides a comprehensive discussion of several known VoIP architectures. (Bellcore, 1-3.) Figure 4-2 of Bellcore (reproduced below) depicts an

exemplary architectural framework for a Voice over Packet (VOP)[3] network. The VOP network of Bellcore includes a set of functional elements: signaling gateway, trunk gateway, routing & translation server, billing agent, call connection agent, service agent, and voice feature servers. (Bellcore, 4-12 to 4-13.) As illustrated in Figure 4-2, these elements are centralized in the VOP network and therefore accessible by multiple customers served through the customer gateways or access gateways.

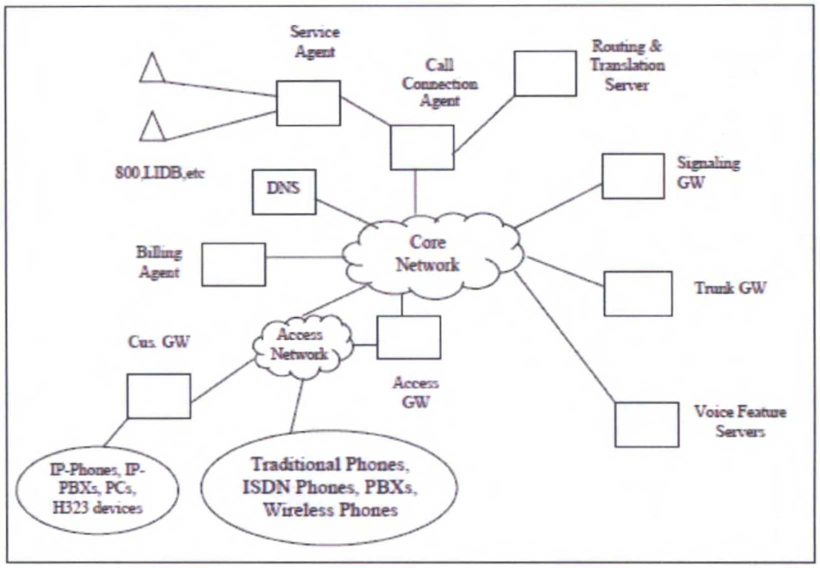


Figure 4-2 VOP Network with Additional Elements and CPE Examples

[3] Bellcore uses the generic term "Voice over Packet" (VOP). Voice over Packet includes packet-based communications protocols such as Voice over Internet Protocol (VoIP).

69. The Core Network of Bellcore "is the packet transport network that provides connectivity to the functional elements in the VOP network." (Bellcore, 4-11.) Figure 4-2 of Bellcore does not illustrate the details of the Core Network. However, Bellcore describes several specific implementations that can be used for the Core Network, including Internet Protocol networks (Bellcore, 5-46) and ATM networks. (Bellcore, 5-52.) Bellcore further explains that several approaches exist for IP over ATM including Classical IP over ATM (CIOA) IETF Multiprotocol Label Switching, LAN emulation (LANE) and the ATM Forum's multiprotocol over ATM (MPOA). Figure 5-11 of Bellcore, reproduced below, illustrates an exemplary classical IP over ATM (CIOA) network that can be used as the core network of Figure 4-2.

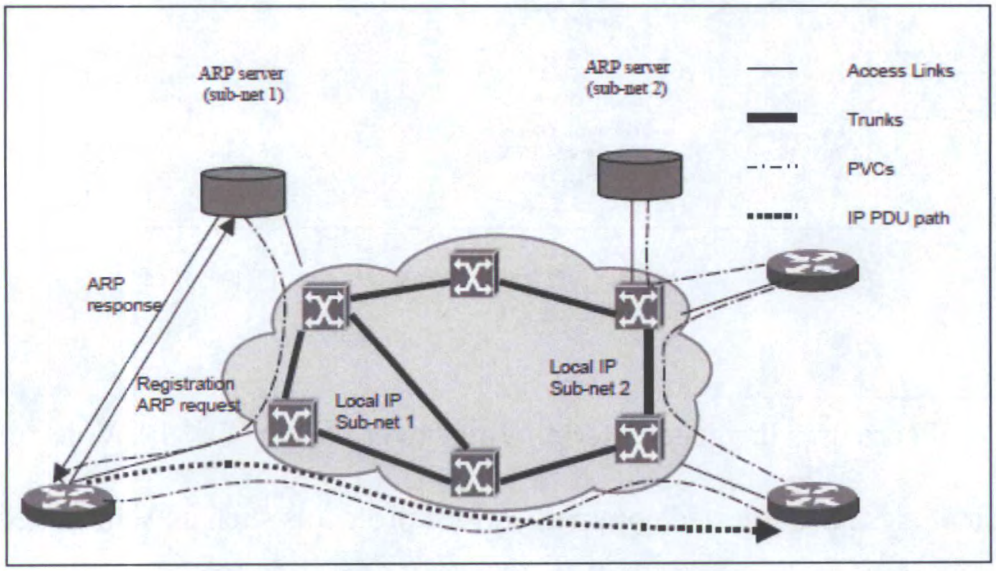


Figure 5-11 CIOA

70. Figure A below incorporates routing elements of the exemplary classical IP over ATM core network of Figure 5-11 into the architecture of Figure 4-2. For ease of description, only a set of routing elements is depicted in Figure A. As would be appreciated by persons of skill in the art, the classical IP over ATM core network shown in Figure A could include additional routing elements and/or address resolution protocol (ARP) servers.

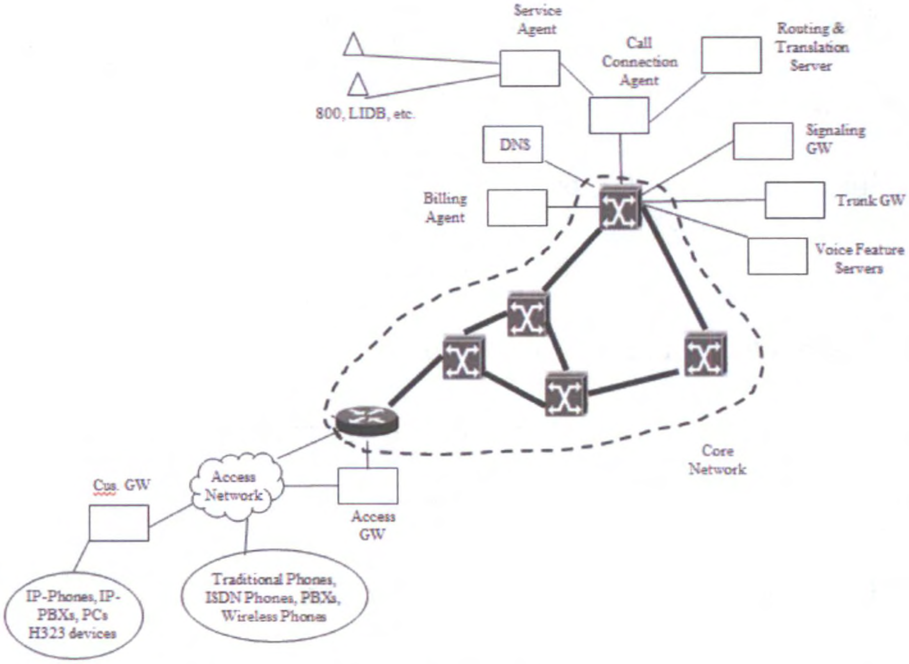


FIGURE A

71. Customers (depicted in the ovals at the bottom of Figure A) connect to the VOP infrastructure via a Customer Gateway or Access Gateway, depending on the type of user equipment at the customer site. This architecture was common, as reflected in Figure 1 of Goode cited by Securus during the IPR of the '167 patent.

(Goode, p. 2.) Goode demonstrates that a customer (*e.g.*, business), uses a gateway device to process VoIP data packets to or from the telephone terminals of the customer for transmission over the core network.

72. Bellcore describes that the target customers for VOP include business customers and residential customers. (Bellcore, 3-1.) Although Bellcore does not explicitly state that a prison facility can be a customer, a person of ordinary skill in the art would understand that, just like other customers, prison facilities would also benefit from using VOP services. In fact, the Patent Owner cited multiple prior art documents during the '167 IPR proceeding establishing that prison facility utilize VoIP technology. For example, the BubbleLink Software architecture document cited by the Patent Owner in the '167 IPR proceeding acknowledges that VoIP was implemented in products and deployed in inmate phone control systems as of its 2003 publication date. (Exhibit GTL 1017, BubbleLink Software architecture, p. 8.) And the Commander II call control system utilized in prison facilities (and referenced in Spadaro) supported VoIP in 2002 as discussed in the Commander II web pages submitted by the Patent Owner in the '167 IPR proceeding. (Exhibit GTL 1025, Commander II, p. 1.) In addition, U.S. Patent No. 8,031,849 to Apple ("Apple") explains that "the application of VOIP principles to the implementation of ICS [inmate communication systems] offer flexibility, added feature functionali-

ty and reduction in operating costs needed to support significant upgrading of existing ICS systems and services." (Exh. 1021, Apple, 6:27-31.)

73. Bellcore explains potential customer motivations for using VOP services: "To save money – the use of VOP services may represent cost savings to the customer" and "For convenient access to new services." (Bellcore, 3-2.) This motivation is echoed by the BubbleLink software architecture document cited by Patent Owner in the '167 IPR that stresses: "Internet protocol (IP) telephony is changing the face of telecommunications. Moreover, it is creating new opportunities for doing business in this dynamic marketplace. Spurred by global deregulation and an increasing demand for value-added services, new operators are eagerly exploiting the flexibility, low cost, and technological potential of the IP network." (BubbleLink, p. 2.) For these reasons, a person of ordinary skill in the art would be motivated to use the VOP architecture of Bellcore with the prison communications functionality of Hodge.

74. Figure 36 of Hodge (reproduced below) illustrates an exemplary prison communications system (the call management system 10). The call management system 101 of Hodge includes a telephone bank 103 having a plurality of user telephones 102. (Hodge, 18:19-27.) Telephone bank 103 is connected to an electronic switchboard device 105. The electronic switchboard device 105 of Hodge "regu-

lates calls and connects them to the proper outgoing trunk 111. Trunk line 111 may consist of a multitude of connections to any number of local, long distance, or international telephone providers." (Hodge, 18:51-55.) The electronic switchboard device 105 of Hodge therefore includes a network gateway device.

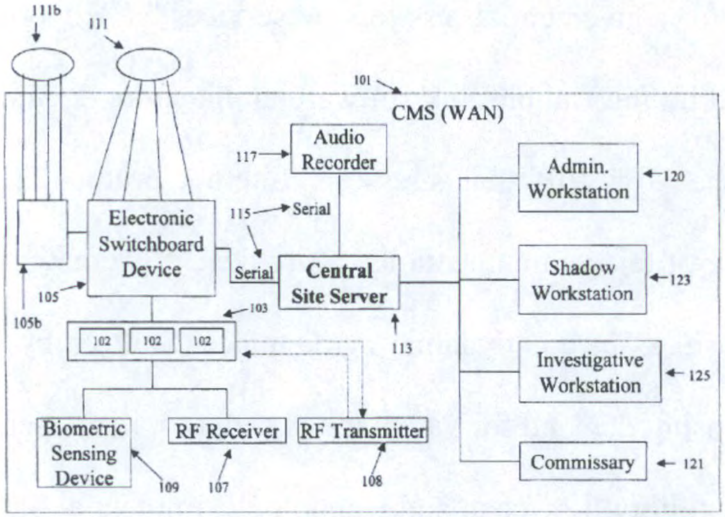


FIG. 36

75. Hodge also describes several functional elements specific to prison customers: a shadow workstation 123, an investigative workstation 125, and a commissary workstation 121. Hodge further describes that these functional elements are integral within the central site server: "Furthermore, administrative workstation 120, shadow workstation 123, investigative workstation 125, and commissary workstation 121 may be integral within the central site server." (Hodge, 21:13-18.) Indeed, Hodge illustrates these elements as directly connected to the central site server. (Hodge, Figure 36.) Hodge indicates that "[i]n WAN configuration, the site

server is connected to multiple switchboard devices that are located in separate institutions." (Hodge, 10:41-43.) That is, the site server and its integral functional elements of Hodge are centralized. Thus, the switchboard is at a facility and would act as an access gateway to connect the telephone devices to the WAN and central site server. In addition, the switch board could connect to other switchboards, some of which could presumably serve as a centralized outlet to the PSTN. (Hodge 50:10-19.) Moreover, in a WAN configuration, Hodge indicates that arbitrary data technologies can be used: "connecting means commonly known in the art for connecting electronic devices." (Hodge, 50:37-45.) At the time of the Hodge patent, the Internet Protocol was a well-established means for connecting electronic devices. This motivates the seeking out of a network architecture such as that proposed by Bellcore.

76. A person of ordinary skill in the art would have been motivated to combine the functional elements of Hodge with the architectural framework of Bellcore because both are in the same field (telecommunications) and address the same problem – centralized control and management of telecommunications across multiple sites.

77. Bellcore also emphasizes the need for network-based account management (*e.g.*, through its LIDB platform), and network-based fraud detection such as provided by the shadow and investigative workstations of Hodge. (Bellcore, 5-73,

85 and 86.) And, Hodge discloses that the switchboard devices can be located at a remote institution. Thus, for these additional reasons, a person of ordinary skill in the art would have been motivated to combine Bellcore with Hodge.

78. Bellcore, like Hodge, centralizes call processing and data management. Both Bellcore and Hodge have the ability to centrally log and record details of all calls placed through the system. (See *e.g.* Bellcore, 5-22, Hodge 10:24-26.) Both Bellcore and Hodge provide for centralized security management (see Bellcore, 5-22, Hodge 21:1-2) Both Bellcore and Hodge centrally store voice announcements/prompts used to interact with users through Interactive Voice Response Units. (*See*, *e.g*., Bellcore 4-13, Hodge 50:54-58.) Both Bellcore and Hodge provide centralized and local account management access restrictions. (*See* Bellcore, 5-85,86, Hodge 41:46-67.) Both Bellcore and Hodge allow for the capability to connect to a live operator at a centralized facility. (*See* Bellcore, 3-3, Hodge 20:42-61.) Both Bellcore and Hodge allow for the use of a debit card platform. (*See*, *e.g*., Bellcore, A-1, Hodge 9:46-48.) Both Bellcore and Hodge collect billing records, CDRs (Call Detail Records), at a central facility. (*See*, *e.g*., Hodge 25:36-43, Bellcore, 4-12.) These synergies would have led a POSITA to incorporate Hodge's inmate management into the existing centralized platform of Bellcore.

79. Additionally, Hodge discloses that its functional elements are configured for use with a number of different wide area network ("WAN") data connec-

tions (Hodge, 50:37-45), and Bellcore provides a VOP architecture (a known example of a WAN data connection) as a specific recommendation. Also, as I discussed above in paragraph 72, customers, including prisons, benefit from VOIP efficiencies, and therefore a POSITA would have been motivated to add a VOIP network to carry Hodge's inmate traffic.

80. Thus, a person of ordinary skill in the art would have been further motivated to combine the functional elements of Hodge with the architectural framework of Bellcore, because the resulting system would have had a reasonable expectation of success. A person of ordinary skill in the art could have combined the functions of Hodge with the architecture of Bellcore by known methods. The results of the combination would have been predictable to a person of ordinary skill in the art.

81. Figure B below edits Figure A to incorporate the centralized functional elements of Hodge (central site server 113, commissary workstation 121, shadow workstation 123 and investigative workstation 125). In addition, Figure A has been edited to illustrate multiple prison facilities as customers, each having a telephone bank 103 with multiple user telephones 102. The telephone bank 103 of Hodge is connected to the VOIP network access gateway of Bellcore. This is equivalent to connecting through the electronic switchboard of Hodge. The '357 patent acknowledges that this network access configuration of telephones coupled to a

VoIP access gateway was known prior to the alleged priority date of the remaining claims of the '357 patent (July 12, 2007):

> Call processing gateways 140 of this preferred embodiment provide conversion of analog signals associated with telephone terminals 141 and visitation telephones 143 and digital data packets of the packet switched network to provide a VoIP gateway … Embodiments of the present invention **utilize commercially available devices**, such the IAD 2400 series of integrated access devices available from Cisco Systems, Inc., San Jose, Calif., **in providing a call processor gateway**.

('357 patent, 7:12-23(emphasis added).) And, this architecture is depicted in references cited by Patent Owner in the '167 IPR such as Goode. (*See, e.g.,* Goode, p. 1.)

82. Figure B is further annotated to illustrate how the combination of Bellcore and Hodge maps to the limitations of the independent claims of the '357 patent.

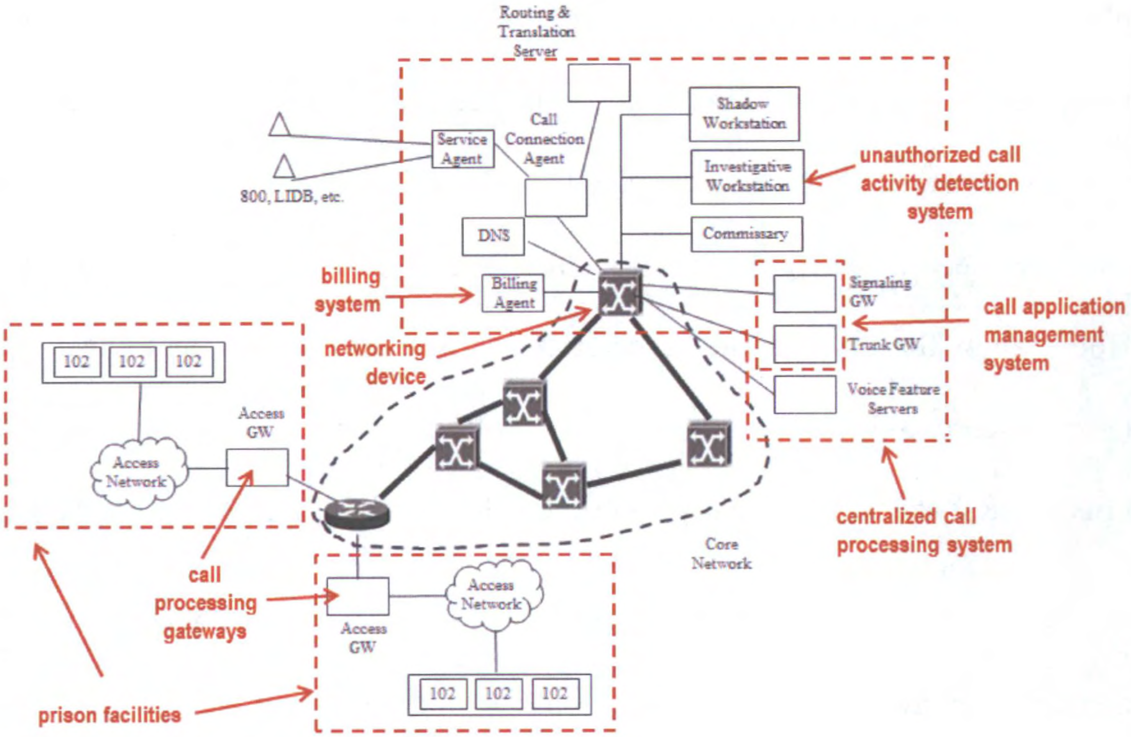


FIGURE B

83. As discussed above, a person of ordinary skill in the art would have been motivated to utilize Bellcore's VoIP architecture with the system of Hodge to take advantage of the low cost and flexibility provided by an IP network. Additionally, a person of ordinary skill in the art would recognize that the call processing and inmate management capabilities would be centralized in the combined system for a number of reasons. First, both Bellcore and Hodge motivate centralization. For example, Bellcore describes centralized logging and recording of calls at its trunking gateway. (Bellcore, 5-22.) Similarly, Hodge discloses that its centralized site server has the "ability to log and record details of all telephone calls

placed through the system." (Hodge, 10:24-26.) Bellcore also describes the centralized voice feature services including announcement servers, IVR units, etc. (Bellcore, 4-13.) Hodge also stores digitized audio used for voice prompts in its centralized cite server. (Hodge, 50:54-58.) As a further example, both Bellcore and Hodge allow for the capability to connect to a live operator at a centralized facility (*See* Bellcore, 3-3, Hodge 20:42-61) and collect billing records, Call Detail Records (CDRs) at a central facility. (*See, e.g.*, Hodge 25:36-43, Bellcore, 4-12.)

84. Second, centralization was a standard technique in communications networks. Many telecommunications services require continuous or near continuous operation. In fact, five "nines" availability (99.999% availability) is the objective of the Bell Operating companies. That is, the goal for these carriers is to have less than 6 minutes of total service downtime in **a year**. The need to retain such a high quality of service requires the equipment to be located in buildings or sites meeting certain exacting design criteria.[4] The Network Equipment-Building System (NEBS) is an example of standardized design guidelines for infrastructure

[4] In most cities in the U.S., it is common to see telephone companies occupy large multi-story buildings housing sometimes enormous amounts of diverse equipment. It is not uncommon for a company to have a dozen or more central offices and their supporting equipment housed in a single building.

supporting telecommunications equipment. For example, buildings housing telecommunications equipment must be designed to address temperature/cooling, humidity, acoustic noise, electromagnetic compatibility, electrostatic discharge, fire prevention and protection, earthquake protection, and office vibrations. (Notes on Networks, 9-25.) Further, the equipment must have access to batteries and/or uninterruptible power systems (UPS) to keep critical equipment operating when commercial power is lost. (Notes on Networks, 9-24.) Also, facilities housing telecommunications equipment, particularly databases having customer information, need security to protect against internal and external intrusions. (*See, e.g.,* Osifchin, p. 2.) Constructing and maintaining these buildings is expensive. (*See, e.g.,* Osifchin, pp. 1-6.) Because of these factors, the cost of housing telecommunications equipment is expensive. Therefore, one major motivation for locating equipment in the same geographic area or location is reducing the cost of the physical infrastructure requires to house and support telecommunications equipment.

85. When equipment is located in the same geographic area or location, communication links between the elements are minimized, which further reduces cost and makes the links less prone to error.

A. The combination of Bellcore and Hodge teaches or suggests each and every limitation recited in independent claims 1 and 10 and corresponding dependent claims 2, 8, 9, 11, 14, 16, and 17 18.

1. Bellcore and Hodge render claim 1 obvious.

86. Because claims 2, 5, 8, and 9 depend from cancelled claim 1, I address the limitations of this claim herein. The combination of Bellcore and Hodge discloses each and every limitation recited in claim 1. Claim 1 is reproduced below. The claim limitations have been labeled for ease of discussion.

> 1. [P] A computer-based system, at a plurality of facilities, for managing inmate information, each of the facilities having one or more telephone terminals and computer terminals, the computer-based system located remotely from at least one of the plurality of facilities, the system comprising:
>
> [A] a networking device exchanging Voice over Internet Protocol (VoIP) data packets with call processing gateways at the plurality of facilities over digital data links, the call processing gateways processing the VoIP data packets to or from the telephone terminals for transmission over the digital data links; **[also referred to as "the 'networking device' limitation"]**
>
> [B] an inmate management-system coupled to the networking device for providing shared data access of inmate records to computer terminals at said plurality of facilities, said inmate records created with first inmate information collected from a first computer terminal at a first facility of the plurality of facilities and modified responsive to collecting second inmate information from

> a second computer terminal at a second facility of the plurality of facilities; and **[also referred to as "the 'inmate management-system' limitation"]**
>
> [C] a call application management system connecting a call to or from the telephone terminals over a telephone carrier network responsive to receiving a request for connecting the call and the call being authorized based on the inmate records provided by the inmate management system. **[also referred to as "the 'call management system' limitation"]**

a) "computer-based system located remotely from at least one of the plurality of facilities." (limitation 1[P])

87. The VOP architecture of Bellcore includes a number of functional elements used to process calls made by customers (*e.g.*, the prison facilities of Hodge) including, among other elements, a call connection agent (CCA), a service agent, voice feature servers, a trunk gateway, a signaling gateway, and a billing agent. (Bellcore, 4-12 to 13.) Bellcore additionally includes centralized data storage (*e.g.*, LIDB, 800 databases). LIDB stores billing options for accounts (*e.g.*, collect, calling card, and bill-to-third). (Ex. 1026, Bellcore Notes on Network, pp. 14-29.) LIDB also contains non-billing information about these accounts such as personal identification number (PIN) and calling name. (*See,* Bellcore Notes on Network, p. 14-35.) As is well-known to a person having ordinary skill in the art, these functional and storage elements are "*computer-based*." Hodge provides additional functional elements – investigative workstation, shadow workstation and commis-

sary workstation (*i.e.*, computers) used to provide call processing. (*See, e.g.*, Hodge, 20:18-21:18.) Bellcore emphasizes the need for network-based fraud detection (*e.g.* Bellcore, 5-73, 5-85, 5-86) so the addition of the investigative functionalities of Hodge to the architecture of Bellcore would have been obvious to a person of ordinary skill in the art. Moreover, as indicated above, Hodge allows for arbitrary data technologies to connect remote sites to a centralized facility. The Bellcore architecture details data technologies to be used for interconnecting remote sites to a centralized facility.

88. As discussed above, and illustrated in Bellcore Figure 4-2 and Figure B, the storage functional elements of both Bellcore and Hodge are "*centralized*" in the network. Centralization of storage and functional elements such as illustrated in Bellcore was a standard practice in the telecommunications industry for decades prior to the alleged priority date of the remaining claims of the '357 patent. Hodge describes that centralization can be applied in the prison context: "In a WAN configuration, the site server is connected to multiple switchboard devices that are located in separate institutions." (Hodge, 10:41-43.) In addition, the switch boards could connect to other switchboards, some of which could presumably serve as a centralized outlet to the PSTN. (Hodge 50:10-19) Thus the central site server and its integral functional elements are centralized, or in other words, located remotely from the telecommunications platforms (switchboard devices) in the prison facili-

ties, but Hodge also allows for some switchboard access to coexist with the central site server.

89. Hodge further discloses that information storage and management can be centralized (located remotely from the facilities). For example, Hodge describes a site server that is "connected to multiple switchboard devices that are located in separate institutions." (Hodge, 10:41-42.) The site server "serves as the database location for the entire system." (Hodge, 10:42-44.) Figure 1 of Hodge shows that several different "workstations" (administrative workstation 120, investigative workstation 125, etc.) can be connected to the central site server 113. These workstations are described as running "software utilizing a GUI (graphical user interface)." (Hodge, 10:49-52.) And, Bellcore discloses centralized account storage and management through its LIDB database. Therefore, a person of ordinary skill in the art would understand that these workstations would be considered to be "*computer terminals*."

90. Hodge describes that "administrative and investigative workstations may be located at every facility" served by the site server, and that these workstations can be "used to create, edit, and monitor user accounts and telephone calls." (Hodge, 10:44-46 and 10:35-37.) Additionally, the call management system 101 of Hodge includes a telephone bank 103 having a plurality of user telephones

102. (Hodge, 18:19-27.) In Hodge, individual facilities have one or more computer terminals. Thus, Hodge discloses that "*each of the facilities*" has "*one or more telephones and computer terminals*."

b) "a networking device exchanging Voice over Internet Protocol (VoIP) data packets with call processing gateways at the plurality of facilities over digital data links." (limitation 1[A])

91. Claim 1 requires "*a networking device exchanging Voice over Internet Protocol (VoIP) data packets with call processing gateways at the plurality of facilities over digital data links*." Hodge discloses digitizing both voice and call information for purposes of "efficient data transfer." (Hodge 19:16-18 and 19:37-40.) Thus, the connection between the prison facilities (Electronic Switchboard Device 105) and the central facility (Central Site Server) is done over digital data links *e.g.* via serial port 15, but Hodge contemplates any type of WAN data connection. Using the Bellcore architecture, the access gateways (AG) (illustrated in Forys Figure B) are the recited "call processing gateways at the plurality of prison facilities." An access gateway (AG) "provides customer access to the VOP network from traditional network access interfaces supported in circuit switched networks." (Bellcore, 5-1.) An access gateway is a VoIP gateway providing "circuit-mode to packet-mode conversion for media streams." (Bellcore, 5-3.)

92. Bellcore does not explicitly disclose that an access gateway is implemented at a prison facility. A person of ordinary skill in the art would recognize that an access gateway would be implemented at a customer site, which may include a prison facility. For example, the access gateway could be utilized in the network gateway functionality provided by the electronic switchboard device 105 of Hodge, which is disclosed to be general enough to handle a multiplicity of data access protocols. This architecture is also disclosed by Spadaro and reflected in the references cited by Patent Owner in the '167 IPR proceeding including the Goode reference. In addition, Apple describes and motivates the placement of access gateways at prison facilities. (Apple, Figures 2, 8 (line interface 210); Figure 5 (FXS gateway 108); Figure 6 (FXS gateway 112/FXO gateway 113.) And the '357 patent itself indicates that access gateways were well-known. ('357 patent, 7:20-23.)

93. The specification refers to the component that exchanges VoIP data packets with the call processing gateways as a router/switch 118. Routers and switches capable of exchanging IP traffic including VoIP traffic were well-known. For example, Cable Labs describes a VoIP infrastructure using routers/switches. Additionally, during the '167 proceeding, Patent Owner cited a prior art document, VoIP by Goode, that describes a system having a gateway exchanging VoIP packets with a router/switch. (Goode, pp. 1-2.)

94. As discussed above and illustrated in Bellcore Figure 5-11 and Figure B, the Core Network of Bellcore may be implemented using a variety of technologies including "classical IP over ATM." (Bellcore, 5-55.) "In classical IP over ATM, IP routers are attached to ATM backbone networks. Switches in the ATM network are treated as devices of IP sub-networks." (Bellcore, 5-55.) Like the router/switch 118 of the '357 patent, a routing element (*e.g.*, an ATM switch) in the Core Network of Bellcore is connected to the centralized call processing elements (*e.g.*, signaling gateway, trunk gateway, billing agent, etc.) and is the recited "*networking device*" as depicted in Figure B-2.

95. The access gateway "provides functions such as packetization" of calls from traditional telephone sets. (*See* Bellcore, 4-12.) That is, the access gateway transmits VoIP packets from the customer (*e.g.*, prison facility of Hodge) over the core network to the routing element (*e.g.*, ATM switch) connected to the centralized call processing components. This architecture is analogous to the architecture shown in Figure 1 of the '357 patent where the call processing gateways connect to a router/switch through a network. The access gateways (*call processing gateways*) therefore process "*the VoIP data packets to or from the telephone terminals for transmission over the digital data links*."

96. The routing element (*e.g.*, ATM switch) in the core network therefore receives VoIP data packets from a plurality of access gateways over a digital link (IP network). Thus, the routing/switching element (*e.g.*, ATM switch) in the core network connected to the centralized call processing components "*exchange[s] Voice over Internet Protocol (VoIP) data packets with call processing gateways at the plurality of facilities over digital data links.*"

c) "an inmate management-system coupled to the networking device for providing shared data access of inmate records to computer terminals at said plurality of facilities, said inmate records created with first inmate information collected from a first computer terminal at a first facility of the plurality of facilities and modified responsive to collecting second inmate information from a second computer terminal at a second facility of the plurality of facilities." (limitation [1B])

97. As described above, the call processing system of Bellcore and Hodge (as highlighted by Figure B, above) is centralized and located remotely from the facilities. For example, Hodge discloses a site server that is "connected to multiple switchboard devices that are located in separate institutions," and that "serves as the database location for the entire system." (Hodge, 10:41-45.) Further, Hodge describes that, at the site server, inmate information is "digitized for efficient data transfer and efficient record keeping." (Hodge, 19:39-40.) This data includes user call information, financial transaction data, call restrictions, PINs, biometric verification data, etc. (*See* Hodge, 19:39-44.) A person of ordinary skill in the art would

have found it obvious to couple Hodge's site server (*inmate management system*) to Bellcore's Core Network (networking device) because the *networking device* accesses inmate information such as PIN information for call authorization functions and because both are centralized. I discussed additional motivations for the combination of Bellcore and Hodge above. Therefore, the combination of Bellcore and Hodge disclose "*an inmate management-system coupled to the networking device for providing shared data access of inmate records to computer terminals at said plurality of facilities*."

98. Hodge also teaches that the creation and modification of inmate records can be performed by different facilities. For example, Hodge discloses that administrative workstations (*e.g.*, computer terminals) may be located "at every facility." (Hodge, 10:46.) These administrative workstations can "**create, edit**, and monitor user accounts and telephone calls." (Hodge, 10:35-37 (emphasis added).) Hodge does not limit which facilities/workstations are permitted to create/edit the inmate records. Hodge discloses that "changes can be made at any of the different institutions and then be applied globally or locally". (Hodge, 10:65-67.) Also, "it is foreseeable that one or more sets of workstations at a central facility may be used to administrate all user accounts." (Hodge, 10:46-48.) Therefore, a person of ordinary skill in the art would understand from Hodge that any of the administrative workstations located at any of the different facilities could create inmate records, and

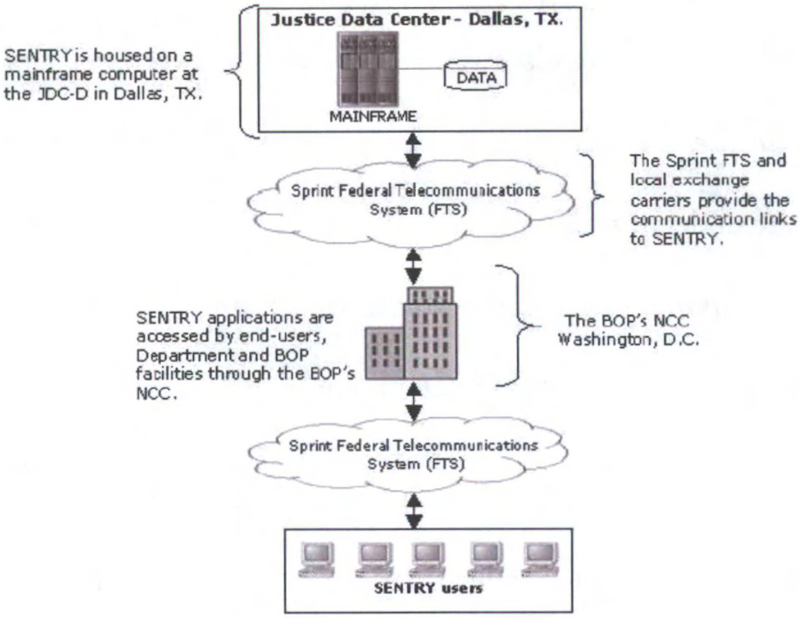
that any of the other workstations at any of the other facilities could edit those records. Further, it is well understood that modifying an existing record is equivalent to creating a new record that includes old unmodified data of the existing record and the new "modifying" data.

99. For example, after a user account has been created at a first facility (as depicted, *e.g.*, in Figure 24 of Hodge), an administrator at a second facility can access an account screen 2400 (via a computer terminal), and by pressing the Change button 2419, "modify data such as user name, living unit, user language preference, status code, and comments." (Hodge, 43:19-21.) Throughout Hodge's specification, Hodge provides several other modifications that can be made to inmate records, without ever restricting the locations at which those changes can be made. This understanding is consistent with Hodge's site server, through which "all inmate and call information" is routed for "efficient data transfer and efficient record keeping." (Hodge, 19:37-40.) Also, Hodge provides for access controls that indicate (and constrain) which prison authorities can have access to which records, ranging from all records in the entire system to only records pertaining to a particular cell block. (Hodge, 35:64-36:32). This includes the ability to "manually modify transactions." Therefore, the combination of Bellcore and Hodge discloses "*said inmate records created with first inmate information collected from a first computer terminal at a first facility of the plurality of facilities and modified responsive to*

collecting second inmate information from a second computer terminal at a second facility of the plurality of facilities."

100. As I discussed above, the centralization of storage and management of inmate data was well-known and routine prior to the July 12, 2007 filing date of the '357 patent. The Federal BOP's SENTRY system provided for shared data access of inmate records to computer terminals at a plurality of prison facilities as illustrated in the Figure from the BOP Audit Report, reproduced below. (Audit Report, p. 3.) SENTRY "resides on a BOP mainframe computer located at the Justice Data Center in Dallas, Texas (JDC-D) operated by the Department of Justice (Department) Justice Management Division's (JMD) Computer Services." (*Id.*, p. 2.) Personal computers "at approximately 200 facilities in the Department and BOP" access SENTRY "by way of the BOP's Washington, D.C., Network Control Center." (*Id.*) "The remote sites include federal correctional facilities, regional offices, Community Corrections Offices (CCO), and other selected offices." (*Id.*, p. 2.) Through this centralized architecture, "SENTRY allows concurrent sharing of data among multiple users." (*Id.*, p. 3.) Thus, SENTRY allowed for inmate records to be created with inmate information collected from a first computer terminal at a first facility and modified responsive to collecting second inmate information from a second computer terminal at a second facility.

SENTRY Network Configuration


Justice Data Center - Dallas, TX.
SENTRY is housed on a mainframe computer at the JDC-D in Dallas, TX.
DATA
MAINFRAME
Sprint Federal Telecommunications System (FTS)
The Sprint FTS and local exchange carriers provide the communication links to SENTRY.
SENTRY applications are accessed by end-users, Department and BOP facilities through the BOP's NCC.
The BOP's NCC Washington, D.C.
Sprint Federal Telecommunications System (FTS)
SENTRY users

d) **"a call application management system connecting a call to or from the telephone terminals over a telephone carrier network responsive to receiving a request for connecting the call and the call being authorized based on the inmate records provided by the inmate management system." (limitation 1[C])**

101. The VOP network of Bellcore includes a trunk gateway and a signaling gateway. (*See* Bellcore, Figure 4-2; Figure B.) The trunk gateway and signaling gateway together provide the functionality of the claimed "*call application management system*."

102. The Trunk Gateway of Bellcore "provides the communications interface between the PSTN and the Core (VOP) network." (Bellcore, 5-18.) The Trunk Gateway includes a module that "performs packetization of audio signals (received

from the PSTN) and depacketization of data (received from the Core network)." (Bellcore, 5-19.) Thus, Trunk Gateway "*connect[s] a call to or from the telephone terminals over a telephone carrier network*." Also, a person having ordinary skill in the art would understand that such call connections are commonly performed "*responsive to receiving a request for connecting the call*," which occurs whenever a caller dials a telephone number at a telephone terminal.

103. In addition, Hodge teaches call authorization based on inmate records. Hodge describes a central site server that "serves as the database location for the entire system." (Hodge, 10:44-45.) Hodge further discloses PIN checking, and states that "[t]he information entered by the user is compared with information stored in the database for that specific user." (Hodge, 11:44-45.) After a predetermined number of failed attempts by the user to enter a correct PIN, "the individual may be denied access to the telephone system and an official may be notified." (Hodge, 11:45-48.) Thus, in Hodge, call authorization is also dependent on inmate records (*e.g.*, a stored PIN code for the inmate).

104. Hodge envisions several other ways in which a call may be authorized or denied based on inmate records. For example, Hodge discloses that calls are only permitted when a minimum amount of funds is available in an inmate account: "In order for a user to place a direct call, a user must have sufficient funds in an

account to pay for at least a three-minute call." (Hodge, 42:3-7.) In addition, Hodge discloses that an inmate may have a blocked or allowed call list that dictates whether a particular number is callable: after entering a telephone number, the system "access[es] a list of telephone numbers that the inmate may not call, or alternatively, the system may access a list of numbers that the inmate is authorized to connect to (*i.e.*, the inmate can only call the numbers appearing on the list)." (Hodge, 3:34-38.) Each of these examples authorizes or denies a particular call based on inmate records. Therefore, Bellcore and Hodge discloses "*a call application management system connecting a call…responsive to…the call being authorized based on the inmate records provided by the inmate management system.*"

2. *The combination of Bellcore and Hodge teaches or suggests the limitations of dependent claims 2, 8 and 9.*

a) Claim 2.

105. Claim 2 (reproduced below) depends from independent claim 1. I understand that the Board previously found that claim 1 was obvious over the combination of Spadaro and Hodge. The combination of Bellcore and Hodge also teaches or suggests each of the limitations of claim 1 as I discussed above. Hodge by itself discloses the subject matter recited in claim 2 which depends from independent claim 1

> The system of claim 1, wherein said inmate records comprise at least one of physical description of inmates, social security numbers of the inmates, driver's license numbers of the inmates, biometric data of the inmates, information related to the arrest of the inmates, and contact information of third parties associated with the inmates.

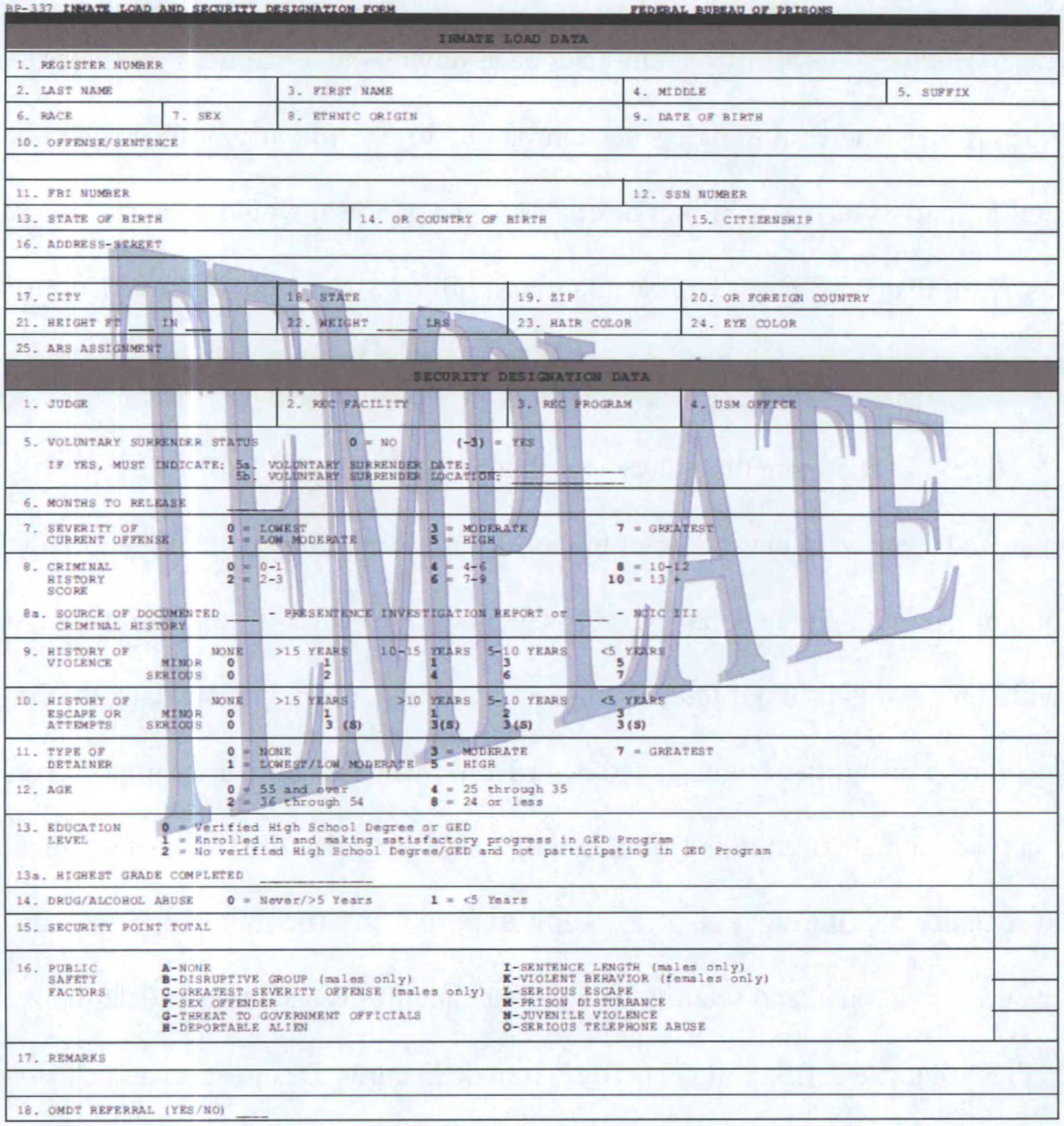
106. The inmate records of Hodge include "*biometric data of the inmates*." Hodge discloses that "biometric data may be required to access the system." (Hodge, 12:18.) The biometric data "may be acquired from users…upon creation of a telephone account for use with the system" and "may be stored along with the user's PIN in the user's account profile or another storage means to be used later as an authentication device." (Hodge, 12:21-28.) Therefore, Hodge discloses that the inmate records can comprise "*biometric data of the inmates*."

107. The inmate records of Hodge also include "*contact information of third parties associated with the inmates*." Hodge discloses that the call processing system "access[es] a list of telephone numbers that the inmate may not call." (Hodge, 3:34-36.) These "blocked" telephone numbers are "*contact information*" belonging to individuals that the inmate is prohibited from contacting, particularly those that the inmate may threaten or harass: "For example, a convicted criminal would be blocked from ever calling his previous victims." (Hodge, 48:51-52.)

108. In addition, Hodge further discloses that an "inmate debit account may alternatively be controlled by the inmate's family…The inmate's family may add funds to the debit account and thereby control the call volume allowed to the inmate." (Hodge, 2:39-46.) It would have been obvious to a person of ordinary skill in the art that where an inmate's account is tied to a third party, information about that third party (such as a billing or other contact address) would be stored in order to provide that third party with account and billing statements and other notifications.

109. I further note that it was well-known and routine to store the type of inmate data recited in claim 2 prior to the July 12, 2007 filing date of the '357 patent. For example, the Federal BOP SENTRY system centrally stored and managed a wide-range of data about federal inmates including general inmate data, the financial responsibility of inmates (court-ordered financial obligations imposed on an inmate), inmate discipline (infraction of institution rules filed against an inmate) and sentence monitoring. (*See*, *e.g.,* Audit Report, p. 2.) The following figure depicts the inmate load and security designation data forms used to populate the SENTRY database. (Exhibit GTL 1022, Inmate Security Designation and Custody Classification Program Statement, p. 41.) As highlighted in this figure, a centralized inmate record stored in SENTRY includes, among other data, the inmate's name, physical description of the inmate (height, weight, hair color, eye color), so-

cial security number of the inmate, offense/sentence, and severity of the offense. (*See,* Program Statement, pp. 26-41.)



TEMPLATE

BP-337 INMATE LOAD AND SECURITY DESIGNATION FORM FEDERAL BUREAU OF PRISONS

INMATE LOAD DATA

1. REGISTER NUMBER			
2. LAST NAME	3. FIRST NAME	4. MIDDLE	5. SUFFIX
6. RACE 7. SEX	8. ETHNIC ORIGIN	9. DATE OF BIRTH	
10. OFFENSE/SENTENCE			
11. FBI NUMBER		12. SSN NUMBER	
13. STATE OF BIRTH	14. OR COUNTRY OF BIRTH	15. CITIZENSHIP	
16. ADDRESS-STREET			
17. CITY	18. STATE	19. ZIP	20. OR FOREIGN COUNTRY
21. HEIGHT FT ___ IN ___	22. WEIGHT _____ LBS	23. HAIR COLOR	24. EYE COLOR
25. ARS ASSIGNMENT			

SECURITY DESIGNATION DATA

1. JUDGE	2. REC FACILITY	3. REC PROGRAM	4. USM OFFICE

5. VOLUNTARY SURRENDER STATUS 0 = NO (-3) = YES

IF YES, MUST INDICATE: 5a. VOLUNTARY SURRENDER DATE: ______________
5b. VOLUNTARY SURRENDER LOCATION: ______________

6. MONTHS TO RELEASE ______

7. SEVERITY OF CURRENT OFFENSE 0 = LOWEST 1 = LOW MODERATE 3 = MODERATE 5 = HIGH 7 = GREATEST

8. CRIMINAL HISTORY SCORE 0 = 0-1 2 = 2-3 4 = 4-6 6 = 7-9 8 = 10-12 10 = 13 +

8a. SOURCE OF DOCUMENTED CRIMINAL HISTORY ____ - PRESENTENCE INVESTIGATION REPORT or ____ - NCIC III

9. HISTORY OF VIOLENCE		NONE	>15 YEARS	10-15 YEARS	5-10 YEARS	<5 YEARS
	MINOR	0	1	1	3	5
	SERIOUS	0	2	4	6	7

10. HISTORY OF ESCAPE OR ATTEMPTS		NONE	>15 YEARS	>10 YEARS	5-10 YEARS	<5 YEARS
	MINOR	0	1	1	2	3
	SERIOUS	0	3 (S)	3(S)	3(S)	3(S)

11. TYPE OF DETAINER 0 = NONE 1 = LOWEST/LOW MODERATE 3 = MODERATE 5 = HIGH 7 = GREATEST

12. AGE 0 = 55 and over 2 = 36 through 54 4 = 25 through 35 8 = 24 or less

13. EDUCATION LEVEL
0 = Verified High School Degree or GED
1 = Enrolled in and making satisfactory progress in GED Program
2 = No verified High School Degree/GED and not participating in GED Program

13a. HIGHEST GRADE COMPLETED ____________

14. DRUG/ALCOHOL ABUSE 0 = Never/>5 Years 1 = <5 Years

15. SECURITY POINT TOTAL

16. PUBLIC SAFETY FACTORS

A-NONE	I-SENTENCE LENGTH (males only)
B-DISRUPTIVE GROUP (males only)	K-VIOLENT BEHAVIOR (females only)
C-GREATEST SEVERITY OFFENSE (males only)	L-SERIOUS ESCAPE
F-SEX OFFENDER	M-PRISON DISTURBANCE
G-THREAT TO GOVERNMENT OFFICIALS	N-JUVENILE VIOLENCE
H-DEPORTABLE ALIEN	O-SERIOUS TELEPHONE ABUSE

17. REMARKS

18. OMDT REFERRAL (YES/NO) ___

b) Claim 8.

110. Claim 8 depends from claim 7 which in turn depends from claim 1. I understand that the Board previously found claim 7 obvious over the combination of Spadaro and Hodge. The combination of Bellcore and Hodge also teaches or suggests each of the limitations of claim 1 as I discussed above. Hodge by itself discloses the subject matter recited in claim 7. Claim 7 is reproduced below.

> The computer-based system of claim 1, wherein the inmate management system is further configured to control access to the inmate records based on logon information received from the computer terminals.

111. *"Control[ling] access to the inmate records based on logon information received from the computer terminals*" was well known long before the filing date of the '357 patent. Using information provided at logon (*e.g.*, password) to control access to a computer system has been a standard way to secure computer systems for decades. (*See, e.g.,* Notes on Network, p. 5-11.) Bellcore stresses the importance of data security in its VOP architecture. (Bellcore 5-85, 86.) Hodge discloses an even more robust approach to data security: Hodge describes "[s]ystem administration software" for institution staff members to customize inmate records. (Hodge, 36:16-17.) However, "only authorized staff members may have access to customize system settings, based on individual staff member security levels." (Hodge, 36:18-20.) The staff member security levels may be "deter-

mined when a user first logs into the system…based upon username and the access level that has been set for each user name by a user manager." The user logs into the system from a computer terminal. (Hodge, 36:21-24.) Hodge's use of the combination of logon credentials and access levels is a technique to control access to the inmate records based on logon information received from the computer terminals.

112. Hodge also discloses the subject matter recited in claim 8 (reproduced below).

> The computer-based system of claim 7, wherein the inmate management system further stores inmate accounts for charging fees to the third parties associated with the inmates for connecting calls placed by the inmates from the plurality of telephone terminals.

113. I note that claim 8 references "the third parties associated with the inmates." The only previous recitation of "third parties associated with the inmates" is in claim 2. However, claim 7 does not depend directly or indirectly from claim 2.

114. The inmate management system of Hodge "*stores inmate accounts for charging fees to the third parties associated with the inmates for connecting calls placed by the inmates from the plurality of telephone terminals.*" Hodge discloses that software of his call processing system "can create a debit account for each us-

er." (Hodge, 11:23-24.) Thus, Hodge discloses establishing an account. Payment for an inmate's call is then "subtracted from the account after its completion." (Hodge, 11:24-26.) Hodge further discloses that a third party can control account funds: "The inmate debit account may alternatively be controlled by the inmate's family…The inmate's family may add funds to the debit account and thereby control the call volume allowed to the inmate." (Hodge, 2:39-46.)

115. It is undisputable that a family member of the inmate is associated with an inmate. Because Hodge's inmate accounts are controlled by the inmate's family and the family adds funds and controls usage, the inmate accounts of Hodge charge fees to third parties associated with the inmate (*e.g.*, family members). These fees are for connecting calls placed by the inmates. Additionally, for these accounts to be used, the accounts must be stored.

c) Claim 9.

116. Hodge discloses the subject matter recited in claim 9 (reproduced below).

> The computer-based system of claim 8, wherein the inmate accounts are charged for expenses incurred by said inmates for an activity other than placing the calls.

117. As I discussed above for claim 8, Hodge discloses inmate accounts that are charged for placing calls. In Hodge, "[i]n addition, or alternatively, an inmate

may be assigned a commissary account." (Hodge, 2:32-34.) That is, Hodge suggests a single account could be used for both calling expenses and commissary expenses. The commissary account acts as the "inmate's general prison spending account" and may thus may be used for expenses other than the placing of telephone calls. (Hodge, 42:3-11.) Hodge explains that as the funds increase in the commissary account "the inmate may apply these funds to the cost of placing telephone calls." (Hodge, 2:34-36.) Thus, in this embodiment, Hodge discloses inmate accounts that are charged for expenses incurred by said inmates for an activity other than placing the calls.

3. Independent Claim 10.

118. Because claims 11, 12, and 14-18 depend from cancelled claim 10, I address the limitations of this claim herein. The combination of Bellcore and Hodge discloses and/or renders obvious each and every feature of claim 10. I again note that claim 10 recites several of the same features as claim 1. Therefore, claim 10 is reproduced below with reference labels that correspond to similarly-recited subject matter of claim 1.

> 10. [P] A method for managing inmate information at multiple facilities including a first facility and a second facility, each facility comprising multiple telephone terminals and computer terminals, the method carried out in a computer-based system located remote-

ly from at least one of the multiple facilities, the method comprising:

[B1] receiving, from a first computer terminal at the first facility, first inmate information associated with an inmate for creating an inmate record;

[B2] receiving, from a second computer terminal at the second facility, second inmate information associated with the inmate for modifying the inmate record;

[B3] storing the inmate record in the computer-based system for shared access across to the inmate record computer terminals in the multiple facilities;

[C1] receiving a request from one of the multiple telephone terminals for connection of a call over a telephone carrier network; and

[C2] connecting the call from one of the telephone terminals over a telephone carrier network and a digital data link responsive to authorizing the call based on the inmate records stored in the computer-based system.

a) "a method for managing inmate information at multiple facilities including a first facility and a second facility, each facility comprising multiple telephone terminals and computer terminals, the method carried out in a computer-based system located remotely from at least one of the multiple facilities." (limitation 10[P])

119. The VOP architecture of Bellcore includes a number of functional elements used to process calls made by customers (*e.g.*, the prison facilities of Hodge) including, among other elements, a call connection agent (CCA), a service

agent, voice feature servers, a trunk gateway, a signaling gateway, and a billing agent. (Bellcore, 4-12 to 13.) As is well-known to a person having ordinary skill in the art, these functional elements are "*computer-based*." Hodge provides additional functional elements – investigative workstation, shadow workstation and commissary workstation (*i.e.*, computers) used to provide call processing. (*See, e.g.,* Hodge, 20:18-21:18.) Bellcore emphasizes the need for network-based fraud detection (*e.g.* Bellcore, 5-73, 5-85, 5-86) so the addition of the investigative functionalities of Hodge to the architecture of Bellcore would have been obvious to a person of ordinary skill in the art. Both Bellcore and Hodge have the ability to centrally log and record details of all calls placed through the system. (*See, e.g.*, Bellcore, 5-22, Hodge, 10:24-26.) Both Bellcore and Hodge provide for centralized security management. (*See,* Bellcore, 5-22, Hodge 21:1-2.) Both Bellcore and Hodge centrally store voice announcements/prompts used to interact with users through Interactive Voice Response Units. (*See, e.g.*, Bellcore, 4-13, Hodge, 50:54-58.) Both Bellcore and Hodge provide centralized and local account management access restrictions. (*See* Bellcore, 5-85 to 86, Hodge 41:46-67.) Both Bellcore and Hodge allow for the capability to connect to a live operator at a centralized facility. (*See* Bellcore, 3-3, Hodge, 20:42-61.) Both Bellcore and Hodge allow for the use of a debit card platform. (*See, e.g.,* Bellcore, A-1, Hodge, 9:46-48.) Both Bellcore and

Hodge collect billing records, CDRs (Call Detail Records), at a central facility. (*See, e.g.*, Hodge, 25:36-43, Bellcore, 4-12.)

120. As discussed above, and illustrated in Bellcore Figure 4-2 and Figure B-2, the functional elements of both Bellcore and Hodge are "*centralized*" in the network. Centralization of functional elements such as illustrated in Bellcore was a standard practice in the telecommunications industry for decades prior to the filing date of the '357 patent as I discussed in detail above. Hodge describes that centralization can be applied in the prison context: "In a WAN configuration, the site server is connected to multiple switchboard devices that are located in separate institutions." (Hodge, 10:41-43.) In addition, the switch board could connect to other switchboards, some of which could presumably serve as a centralized outlet to the PSTN. (Hodge 50:10-19) Thus the central site server and its integral functional elements are centralized, or in other words, located remotely from the telecommunications platforms (switchboard devices) in the prison facilities, although Hodge allows for switchboards to coexists with the central servers.

121. Hodge explicitly discloses a centralized system for "managing inmate information." For example, Hodge describes a site server that is "connected to multiple switchboard devices that are located in separate institutions." (Hodge, 10:41-42.) The site server "serves as the database location for the entire system."

(Hodge, 10:42-44.) Figure 1 of Hodge illustrates that several different "workstations" (administrative workstation 120, investigative workstation 125, etc.) can be connected to the central site server 113. These workstations are described as running "software utilizing a GUI (graphical user interface)." (Hodge, 10:49-52.) Therefore, a person of ordinary skill in the art would understand that these workstations could be "*computer terminals*."

122. Hodge describes that "administrative and investigative workstations may be located at every facility" served by the site server, and that these workstations can be "used to create, edit, and monitor user accounts and telephone calls." (Hodge, 10:44-46 and 10:35-37.) Additionally, the call management system 101 of Hodge includes a telephone bank 103 having a plurality of user telephones 102. (Hodge, 18:19-27.) In Hodge, individual facilities have one or more computer terminals. Thus, Hodge discloses that "*each facility*" has "*multiple telephone terminals and computer terminals*."

b) "receiving, from a first computer terminal at the first facility, first inmate information associated with an inmate for creating an inmate record." (limitation 10[B1])

123. I note that this claim limitation corresponds, in part, to limitation [B] of claim 1. Again, Hodge discloses a site server that is "connected to multiple switchboard devices that are located in separate institutions," and that "serves as the da-

tabase location for the entire system." (Hodge, 10:41-45.) At the site server, inmate information is "digitized for efficient data transfer and efficient record keeping." (Hodge, 19:39-40.) This data includes user call information, financial transaction data, call restrictions, PINs, biometric verification data, etc. (*See* Hodge, 19:39-44.) Hodge further discloses that "[a]ll inmate and call information is routed through central site server 113." Therefore, Hodge discloses receiving information.

124. Hodge also teaches that this information can be "user accounts" created by workstations at the various facilities: administrative workstations (*e.g.*, computer terminals) can "**create, edit**, and monitor user accounts and telephone calls." (Hodge, 10:35-37 (emphasis added).) Therefore, Hodge discloses "*receiving, from a first computer terminal at the first facility, first inmate information…for creating an inmate record.*"

c) "receiving, from a second computer terminal at the second facility, second inmate information associated with the inmate for modifying the inmate record." (limitation 10[B2])

125. I note that this claim limitation corresponds, in large part, to limitation [B] of claim 1. Again, Hodge discloses a site server that is "connected to multiple switchboard devices that are located in separate institutions," and that "serves as the database location for the entire system." (Hodge, 10:41-45.) At the site server, inmate information is "digitized for efficient data transfer and efficient record

keeping." (Hodge, 19:39-40.) This data includes user call information, financial transaction data, call restrictions, PINs, biometric verification data, etc. (*See,* Hodge, 19:39-44.)

126. In the example provided above, Hodge discloses that the inmate record can be that of a user account created by an administrative workstation at one of the facilities. Hodge indicates that these administrative workstations are permitted to do more than simply create their own records: administrative workstations (*e.g.*, computer terminals) can "create, **edit**, and monitor user accounts and telephone calls." (Hodge, 10:35-37 (emphasis added).) Further, Hodge does not limit which facilities/workstations are permitted to create/edit the inmate records. Hodge discloses that "changes can be made at any of the different institutions and then be applied globally or locally". (Hodge, 10:65-67.) Also, "it is foreseeable that one or more sets of workstations at a central facility may be used to administrate all user accounts." (Hodge 10:46-48.) Also, Hodge discloses that "all inmate and call information" for "efficient data transfer and efficient record keeping." (Hodge, 19:37-40.) Therefore, Hodge discloses receiving "*second inmate information associated with the inmate for modifying the inmate record*" "*from a second computer terminal at the second facility*."

d) “storing the inmate record in the computer-based system for shared access across to the inmate record computer terminals in the multiple facilities.” (limitation [B3])

127. I note that this limitation, at least in some part, corresponds to the subject matter of limitation [B] of claim 1. Again, Hodge discloses a site server that is “connected to multiple switchboard devices that are located in separate institutions,” and that “serves as the database location for the entire system.” (Hodge, 10:41-45.) At the site server, inmate information is “digitized for efficient data transfer and efficient record keeping.” (Hodge, 19:39-40.) Therefore, Hodge discloses “*storing the inmate record in the computer-based system*.”

128. As discussed above, Hodge discloses that administrative workstations may be located “at every facility.” (Hodge, 10:46.) These administrative workstations can “**create, edit**, and monitor user accounts and telephone calls.” (Hodge, 10:35-37 (emphasis added).) Hodge does not limit which facilities/workstations are permitted to create/edit the inmate records. Hodge discloses that “changes can be made at any of the different institutions and then be applied globally or locally”. (Hodge, 10:65-67.) Also, “it is foreseeable that one or more sets of workstations at a central facility may be used to administrate all user accounts.” (Hodge 10:46-48.) Therefore, Hodge discloses that the records are stored “*for shared access across to the…computer terminals in the multiple facilities*.”

e) "receiving a request from one of the multiple telephone terminals for connection of a call over a telephone carrier network." (limitation 10[C1])

129. The VOP network of Bellcore includes a trunk gateway and a signaling gateway. (*See* Bellcore, Figure 4-2; Figure B-2.) The Trunk Gateway of Bellcore "provides the communications interface between the PSTN and the Core (VOP) network." (Bellcore, 5-18.) The Trunk Gateway includes a module that "performs packetization of audio signals (received from the PSTN) and depacketization of data (received from the Core network)." (Bellcore, 5-19.) A person having ordinary skill in the art would understand that call connections, such as those made by Bellcore's system, are commonly performed responsive to " *receiving a request…for connection of a call*," which occurs whenever a caller dials a telephone number at a telephone terminal.

f) "connecting the call from one of the telephone terminals over a telephone carrier network and a digital data link responsive to authorizing the call based on the inmate records stored in the computer-based system" (limitation 10[C2])

130. The VOP network of Bellcore includes a trunk gateway and a signaling gateway. (*See,* Bellcore, Figure 4-2; Figure B-2.) The Trunk Gateway of Bellcore "provides the communications interface between the PSTN and the Core (VOP) network." (Bellcore, 5-18.) The Trunk Gateway includes a module that "performs packetization of audio signals (received from the PSTN) and depacketization of da-

ta (received from the Core network)." (Bellcore, 5-19.) As is well-known in the art, a VOP network moves digital data packets, and therefore uses digital data links for communication.

131. Hodge describes a central site server that "serves as the database location for the entire system." (Hodge, 10:44-45.) Hodge further discloses PIN checking, and states that "[t]he information entered by the user is compared with information stored in the database for that specific user." (Hodge, 11:44-45.) After a predetermined number of failed attempts by the user to enter a correct PIN, "the individual may be denied access to the telephone system and an official may be notified." (Hodge, 11:45-48.) Thus, in Hodge, call authorization is also dependent on inmate records (*e.g.*, a stored PIN code for the inmate).

132. Hodge envisions several other ways in which a call may be authorized or denied based on inmate records. For example, Hodge discloses that calls are only permitted when a minimum amount of funds is available in an inmate account: "In order for a user to place a direct call, a user must have sufficient funds in an account to pay for at least a three-minute call." (Hodge, 42:3-7.) In addition, Hodge discloses that an inmate may have a blocked or allowed call list that dictates whether a particular number is callable: after entering a telephone number, the system "access[es] a list of telephone numbers that the inmate may not call, or alterna-

tively, the system may access a list of numbers that the inmate is authorized to connect to (*i.e.*, the inmate can only call the numbers appearing on the list)." (Hodge, 3:34-38.) Each of these examples authorizes or denies *multiple telephone terminals and* a particular call based on inmate records.

g) Claim 11.

133. Claim 11 (reproduced below) depends from independent claim 10. I understand that the Board previously found claim 10 unpatentable over the combination of Spadaro and Hodge. I explained above that Bellcore and Hodge also teaches or suggests the limitations of claim 10. Hodge by itself discloses the subject matter recited in claim 11.

> The method of claim 10, wherein said first inmate information is received upon said inmate's arrest.

134. I note that in the background section of the specification, the '357 patent acknowledges that receiving information about an inmate upon the inmate's arrest was known in the art. Specifically, "[t]he arresting officer may then complete some paperwork identifying the individual, describing the reason for arrest or detention." ('357 patent 2:4-7.) Hodge also suggests this timing limitation.

135. Hodge discloses that the "*first inmate information is received upon [the] inmate's arrest.*" Hodge discloses that "telephone communication systems in

penal institutions provide an inmate **with a telephone account upon arrival**." (Hodge, 2:23-25 (emphasis added).) A person having ordinary skill in the art would have understood that certain inmate information—*e.g.*, inmate's name, account number, PIN number, and telephone numbers of the inmate's friends, family, and/or attorney—would be needed to establish an inmate's telephone account.

136. Hodge discloses a centralized call processing system that is not limited to use in a prison facility, but also can be used to serve other types of facilities. (*See* Hodge, 17-24.) For example, Hodge discloses that his system can be used in any "controlled institutional environment" in which there is a "need to monitor, control, record and provide detailed records of the usage of a telephone system" such as "penal institutions, military institutions, hospitals, schools, businesses, or specific types of government institutions." (Hodge, 1:17-24.) A police station, where a person is **arrested**, is such a controlled environment, and is also a government institution. Indeed, individuals will frequently turn themselves in (*e.g.*, submit to being arrested) at a police station facility. Therefore, a person of ordinary skill in the art would have understood that existing inmate data management systems described in Hodge (as well as in the SENTRY documentation) could be used to service a police station or other similar facility, and that a telephone account could be provided to a person upon his "arrival" (*e.g.*, arrest) at that location. As would be known to a POSITA (or even a lay person), an individual could surrender

at a police station. (*See, e.g.,* Exhibit 1032, LAPD April 24, 2002 News Release.) In such cases, an inmate's arrival at a facility is equivalent to his or her arrest. And as even a lay person would appreciate, an inmate would have a great need for access to a telephone just after his or her arrest.

h) Claim 14.

137. I understand that the Board previously found that claim 10 was obvious over the combination of Spadaro and Hodge. The combination of Bellcore and Hodge also teaches or suggests each of the limitations of claim 10 as I discussed above. Hodge by itself discloses the subject matter recited in claim 14 which depends from independent claim 10:

> The method of claim 10, wherein said inmate record comprises at least one of physical description of the inmate, social security number of the inmate, driver's license number of the inmate, biometric data of the inmate, information related to arrest of the inmate, and contact information of third party associated with the inmate.

138. The inmate records of Hodge include "*biometric data of the inmate.*" Hodge discloses that "biometric data may be required to access the system." (Hodge, 12:18.) The biometric data "may be acquired from users…upon creation of a telephone account for use with the system" and "may be stored along with the user's PIN in the user's account profile or another storage means to be used later as

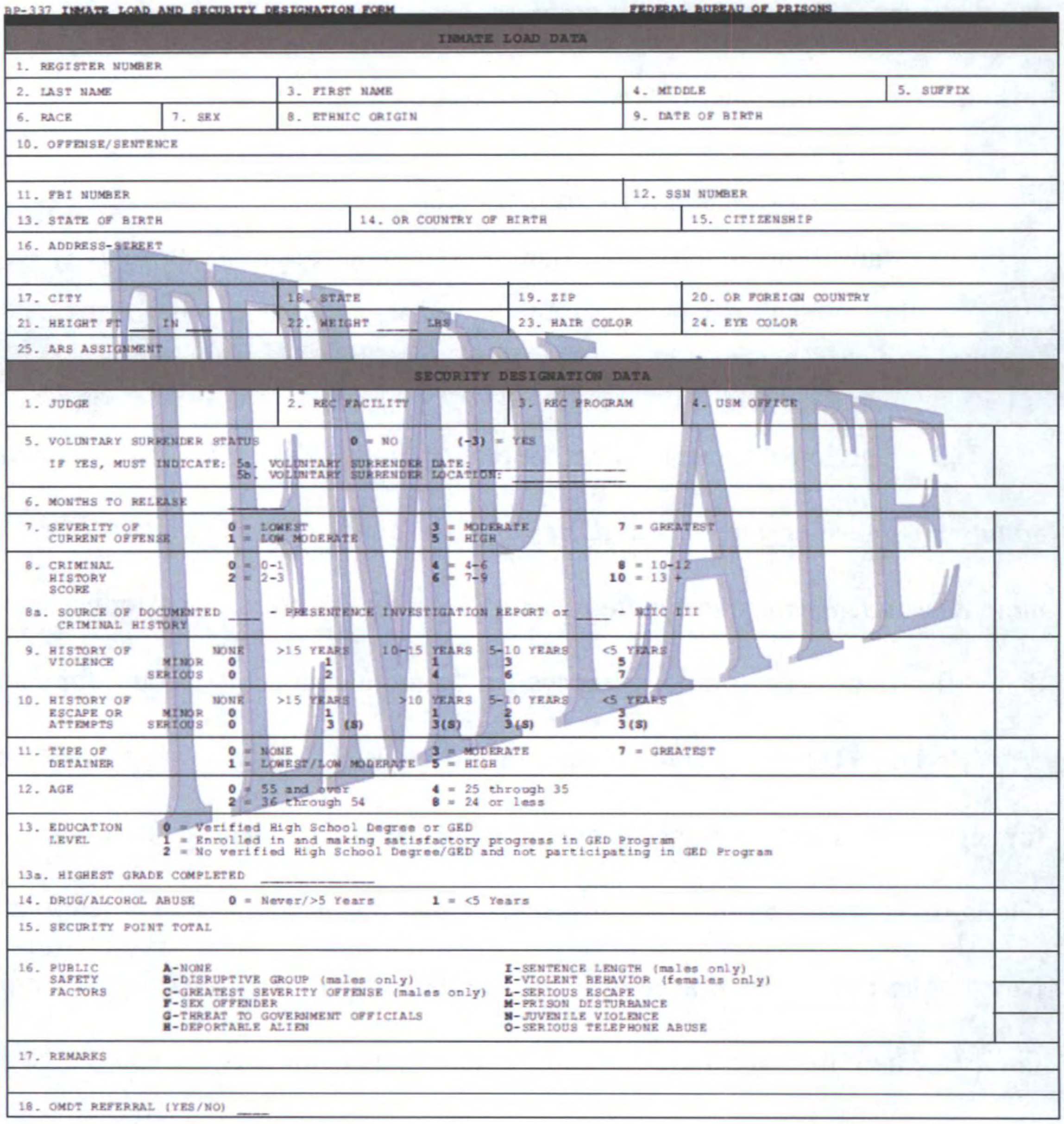
an authentication device." (Hodge, 12:21-28.) Therefore, Hodge discloses that the inmate records can comprise "*biometric data of the inmate*."

139. The inmate records of Hodge also include "*contact information of third party associated with the inmate*." Hodge discloses that the call processing system "access[es] a list of telephone numbers that the inmate may not call." (Hodge, 3:34-35.) These "blocked" telephone numbers are "*contact information*" belonging to individuals that the inmate is prohibited from contacting, particularly those that the inmate may threaten or harass: "For example, a convicted criminal would be blocked from ever calling his previous victims." (Hodge, 48:51-52.)

140. In addition, Hodge further discloses that an "inmate debit account may alternatively be controlled by the inmate's family…The inmate's family may add funds to the debit account and thereby control the call volume allowed to the inmate." (Hodge, 2:39-46.) It would have been obvious to a person of ordinary skill in the art that where an inmate's account is tied to a third party, information about that third party (such as a billing or other contact address) would be stored in order to provide that third party with account and billing statements and other notifications.

141. I further note that it was well-known and routine to store the type of inmate data recited in claim 14 prior to the July 12, 2007 filing date of the '357 pa-

tent. For example, SENTRY centrally stored and managed a wide-range of data about federal inmates including general inmate data, the financial responsibility of inmates (court-ordered financial obligations imposed on an inmate), inmate discipline (infraction of institution rules filed against an inmate) and sentence monitoring. (*See*, *e.g.,* SENTRY Audit Report, p. 2.) The following figure depicts the inmate load and security designation data forms used to populate the SENTRY database. (Exhibit GTL 1022, SENTRY Program Statement, p. 41.) As highlighted in this figure, a centralized inmate record stored in SENTRY includes, among other data, the inmate's name, physical description of the inmate (height, weight, hair color, eye color), social security number of the inmate, offense/sentence, and severity of the offense. (*See,* SENTRY Program Statement, pp. 26-41.)



BP-337 INMATE LOAD AND SECURITY DESIGNATION FORM FEDERAL BUREAU OF PRISONS

TEMPLATE

INMATE LOAD DATA

1. REGISTER NUMBER			
2. LAST NAME	3. FIRST NAME	4. MIDDLE	5. SUFFIX
6. RACE 7. SEX	8. ETHNIC ORIGIN	9. DATE OF BIRTH	
10. OFFENSE/SENTENCE			
11. FBI NUMBER		12. SSN NUMBER	
13. STATE OF BIRTH	14. OR COUNTRY OF BIRTH	15. CITIZENSHIP	
16. ADDRESS-STREET			
17. CITY	18. STATE	19. ZIP	20. OR FOREIGN COUNTRY
21. HEIGHT FT ___ IN ___	22. WEIGHT _____ LBS	23. HAIR COLOR	24. EYE COLOR
25. ARS ASSIGNMENT			

SECURITY DESIGNATION DATA

1. JUDGE	2. REC FACILITY	3. REC PROGRAM	4. USM OFFICE

5. VOLUNTARY SURRENDER STATUS 0 = NO (-3) = YES
IF YES, MUST INDICATE: 5a. VOLUNTARY SURRENDER DATE: ____________
5b. VOLUNTARY SURRENDER LOCATION: ____________

6. MONTHS TO RELEASE ______

7. SEVERITY OF CURRENT OFFENSE 0 = LOWEST 1 = LOW MODERATE 3 = MODERATE 5 = HIGH 7 = GREATEST

8. CRIMINAL HISTORY SCORE 0 = 0-1 2 = 2-3 4 = 4-6 6 = 7-9 8 = 10-12 10 = 13 +

8a. SOURCE OF DOCUMENTED CRIMINAL HISTORY ___ - PRESENTENCE INVESTIGATION REPORT or ___ - NCIC III

9. HISTORY OF VIOLENCE

	NONE	>15 YEARS	10-15 YEARS	5-10 YEARS	<5 YEARS
MINOR	0	1	1	3	5
SERIOUS	0	2	4	6	7

10. HISTORY OF ESCAPE OR ATTEMPTS

	NONE	>15 YEARS	>10 YEARS	5-10 YEARS	<5 YEARS
MINOR	0	1	1	2	3
SERIOUS	0	3 (S)	3(S)	3(S)	3(S)

11. TYPE OF DETAINER 0 = NONE 1 = LOWEST/LOW MODERATE 3 = MODERATE 5 = HIGH 7 = GREATEST

12. AGE 0 = 55 and over 2 = 36 through 54 4 = 25 through 35 8 = 24 or less

13. EDUCATION LEVEL
0 = Verified High School Degree or GED
1 = Enrolled in and making satisfactory progress in GED Program
2 = No verified High School Degree/GED and not participating in GED Program

13a. HIGHEST GRADE COMPLETED ____________

14. DRUG/ALCOHOL ABUSE 0 = Never/>5 Years 1 = <5 Years

15. SECURITY POINT TOTAL

16. PUBLIC SAFETY FACTORS
A-NONE
B-DISRUPTIVE GROUP (males only)
C-GREATEST SEVERITY OFFENSE (males only)
F-SEX OFFENDER
G-THREAT TO GOVERNMENT OFFICIALS
H-DEPORTABLE ALIEN
I-SENTENCE LENGTH (males only)
K-VIOLENT BEHAVIOR (females only)
L-SERIOUS ESCAPE
M-PRISON DISTURBANCE
N-JUVENILE VIOLENCE
O-SERIOUS TELEPHONE ABUSE

17. REMARKS

18. OMDT REFERRAL (YES/NO) ___

i) Claim 16.

142. Claim 16 depends from Claim 14 which in turn depends from claim 10. I understand that the Board previously found claim 16 obvious over the combination of Spadaro and Hodge. Hodge by itself discloses the subject matter recited in

claim 16. Thus, the combination of Bellcore and Hodge also teaches or suggests this claim limitation. Claim 16 is reproduced below.

> The method of claim 14, further comprising:
> establishing an inmate account for charging fees to the third party for connecting calls placed by the inmate associated with the inmate account.

143. The inmate management system of Hodge "*establish[es]an inmate accounts for charging fees to the third party for connecting calls placed by the inmate associated with the inmate account*." As discussed above, Hodge discloses that software of his call processing system "can create a debit account for each user." (Hodge, 11:23-24.) Thus, Hodge discloses establishing an account. Payment for an inmate's call is then "subtracted from the account after its completion." (Hodge, 11:24-26.) Hodge further discloses that this account can be tied to a third party: "The inmate debit account may alternatively be controlled by the inmate's family…The inmate's family may add funds to the debit account and thereby control the call volume allowed to the inmate." (Hodge, 2:39-46.) It is undisputable that a family member of the inmate is associated with an inmate. Because Hodge's inmate accounts are controlled by the inmate's family and the family adds funds and controls usage, the inmate accounts of Hodge charge fees to third parties associated with the inmate (*e.g.*, family members). These fees are for connecting calls

placed by the inmates. Additionally, for these accounts to be used, the accounts must be stored

j) Claim 17.

144. Hodge discloses the subject matter recited in claim 17. Claim 17 is reproduced below.

> The method of claim 16, further comprising: charging said inmate account for an expense incurred by said inmate for an activity other than placing the calls.

145. As I discussed above for claim 14, Hodge discloses inmate accounts that are charged for placing calls. In Hodge, "[i]n addition, or alternatively, an inmate may be assigned a commissary account." (Hodge, 2:32-34.) The commissary account acts as the "inmate's general prison spending account." (Hodge, 42:3-11.) Hodge explains that as the funds increase in the commissary account "the inmate may apply these funds to the cost of placing telephone calls." (Hodge, 2:34-36.) Thus, in this embodiment, Hodge discloses inmate accounts that are charged for expenses incurred by said inmates for an activity other than placing the calls.

B. Bellcore, Hodge and Boykin

146. Hodge discloses that "[i]t is common to utilize a controlled telephone system capable of monitoring outgoing telephone connections in **many types of institutional environments**, such as, but not limited to, penal institutions, military

institutions, hospitals, schools, businesses, or specific types of government institutions." (Hodge, 1:21-33 (emphasis added).) Although Hodge does not expressly disclose that a facility is a "*mobile police station*." Boykin provides this limitation.

147. Like Hodge, Boykin is also directed to acquiring and sharing data associated with a person in a controlled environment. For example, Boykin describes "an effective and efficient method for capturing, transmitting, and storing potential evidentiary video and related information in mobile environments." (Boykin, 1:47-50.) Boykin is specifically directed to the unique scenario in which the "inmate" is in transit, such as in a police vehicle. I note that the '357 patent acknowledges that a police vehicle is a mobile police station. (*See, e.g.,* '357 patent, 15:28-30.)

148. A person of ordinary skill in the art could have combined the mobile facility of Boykin with the system of Bellcore and Hodge using known networking techniques (*e.g.*, wireless routing). Adding a new facility to the known networking techniques (*e.g.,* wireless routing). A POSITA in July 2007 would have been aware of the various wireless communications standards in use (e.g., 802.11). The POSITA would have been able to apply those standardized networking techniques to a mobile workstation. Indeed, laptop computers with wi-fi capabilities were commonplace in 2007. Adding a new facility to the multi-facility infrastructure of

Bellcore and Hodge would therefore have been routine and the results of the combination would have been predictable to a person of ordinary skill in the art.

1. Claim 5.

149. Boykin discloses the subject matter recited in claim 5. Claim 5 is reproduced below.

> The computer-based system of claim 1, wherein said plurality of facilities comprise a mobile police station.

150. Boykin describes "an effective and efficient method for capturing, transmitting, and storing potential evidentiary video and related information in mobile environments." (Boykin, 1:47-50.) In Boykin, a mobile server is also provided for "integrating and storing the captured information in the vehicle" as well as for "transmitting the captured information from the vehicle to a second location, such as a building." (Boykin, 1:57-60.) Boykin describes many different mobile environments in which his system can be employed, including "police, fire, and rescue vehicles." (Boykin, 2:15-17.) The '357 patent acknowledges that a police vehicle is "*a mobile police station*." (*See, e.g.,* '357 15:28-30.)

151. Further, a person of ordinary skill in the art would recognize that any type of facility could use and benefit from centralized data and call management systems. Essentially, so long as a particular facility is able to establish a viable

connection with the centralized system, the centralized system will be capable of supporting that facility. In the above example, Boykin indicates that the mobile environment is capable of transmitting captured data to "a second location, such as a building." A person of ordinary skill in the art would understand that this capability would equally enable the mobile environment to transmit the data to the centralized location, either directly or via the second location. Therefore, Bellcore and Hodge in combination with Boykin disclose using a mobile environment, such as a mobile police station, as a facility to be served by the centralized data and call management system.

2. Claim 12.

152. Boykin discloses the subject matter recited in claim 12. Claim 12 is reproduced below.

> The method of claim 11, wherein said first facility comprises a mobile police station.

153. In Boykin, a mobile server is also provided for "integrating and storing the captured information in the vehicle" as well as for "transmitting the captured information from the vehicle to a second location, such as a building." (Boykin, 1:57-60.) Boykin describes many different mobile environments in which his system can be employed, including "police, fire, and rescue vehicles." (Boykin, 2:15-17.) A police vehicle is "*a mobile police station*."

154. In the above example, Boykin indicates that the mobile environment is capable of transmitting captured data to "a second location, such as a building." A person of ordinary skill in the art would understand that this capability would equally enable the mobile environment to transmit the data to the centralized location, either directly or via the second location. Therefore, Bellcore and Hodge in combination with Boykin disclose using a mobile environment, such as a mobile police station, as a facility to be served by the centralized data and call management system.

C. Bellcore, Hodge and Nguyen.

155. Hodge discloses that the call processing system "access[es] a list of telephone numbers that the inmate may not call." (Hodge, 3:34-35.) These "blocked" telephone numbers belong to individuals that the inmate is prohibited from contacting, particularly those that the inmate may threaten or harass: "For example, a convicted criminal would be blocked from ever calling his previous victims." (Hodge, 48:51-52.) A person having ordinary skill in the art would understand from Hodge that protecting victims and other targeted individuals is an important goal, and is one that could be achieved with additional protections. Although Hodge does not expressly disclose "*notifying said third party of said inmate's arrest based on the contact information*" (claim 15) or "*notifying said third party of transfer of the in-*

mate from one facility of the multiple facilities to another facility of the multiple facilities" (claim 18), these limitations are disclosed by Nguyen.

156. Nguyen is directed to "a system and method for alerting the victims of the change of status of a defendant in the criminal justice system." (Nguyen, 1:7-9.) Nguyen emphasizes the rights and protections of victims: "The rights of victims in the criminal justice system is receiving considerable attention today in the midst of a significant violent crime rate and early release of many offenders due to the over crowding of prisons." (Nguyen, 1:10-13.)

157. Nguyen discloses that a "'Registered Victim' shall be **any person who has provided the system with his or her unique identifying communication address such as a telephone number or electronic address and selected a personal identifying number, i.e., a 'PIN'**." (Nguyen, 3:8-11 (emphasis added).) Thus, Nguyen anticipates the application of its notification system to any person that provides the system with their contact information. Therefore, a person of ordinary skill in the art would have found it obvious to apply Nguyen's notification system to third parties who have an interest in the inmate's status. It would further have been obvious to a person of ordinary skill in the art that family members of the inmate have a strong interest in the status of their relative inmates. A person of ordinary skill would have modified Hodge's central site server to provide notifica-

tions to third parties as taught by Nguyen because both solve related problems arising from the changing status of inmates. And a person of ordinary skill would have modified Hodge to provide the notification feature with a reasonable expectation of success, given that Hodge and Nguyen employ common, well-understood systems to achieve predictable results. Consequently, a person of ordinary skill in the art would have found it obvious to employ Nguyen's status notification system to update family members of the status of the inmate.

1. Claim 15

158. Nguyen discloses the subject matter of claim 15. Claim 15 is reproduced below.

> The method of claim 14, further comprising:
> notifying said third party of said inmate's arrest based on the contact information.

159. Nguyen describes that many different status changes can trigger victim notification: "Many states have passed legislation enacting the right of victims to be alerted to the early release **or other changes in status of defendants**." (Nguyen, 1:13-16 (emphasis added).) Arrest of an inmate would easily have been understood by a person of ordinary skill in the art as constituting such "other changes in status" that would warrant notification to a victim. For example, the arrest of an inmate would require notification to the victim for the same reason as the inmate

being released – the inmate's arrest has an appreciable impact on the safety and/or well-being of the victim. Further, because Nguyen defines victims so as to encompass all who would provide their contact information, it would have been obvious to a person of ordinary skill in the art that other interested third parties (*e.g.*, family members) would be suitable candidates for receiving inmate status notifications.

160. Nguyen further describes a "control station" that functions substantially similarly to Hodge's central site server, by maintaining data records of various inmates: "The system itself includes a central processor or control station for storing in a data base information pertaining to a plurality of prison inmates and a plurality of victims." (Nguyen, 1:55-58.) Upon being informed of the inmate's change in status, the control station "automatically calls and informs the victim of the change." (Nguyen, 2:3-5.)

2. Claim 18

161. The combination of Hodge and Nguyen discloses the subject matter of claim 18. Claim 18 is reproduced below.

> The method of claim 16, further comprising:
>
> notifying said third party of transfer of the inmate from one facility of the multiple facilities to another facility of the multiple facilities; and

establishing another inmate account associated with said third party responsive to transferring the inmate to the other facility.

162. As discussed above, Nguyen describes that victims have "the right…to be alerted to the early release **or other changes in status of defendants**." (Nguyen, 1:13-16 (emphasis added).) A transfer of an inmate would easily have been understood by a person of ordinary skill in the art as constituting such "other changes in status" that would warrant notification to a victim. For example, a transfer of the inmate to a facility within the vicinity of his victim would require notification to the victim for the same reason as the inmate being released – the inmate's status has an appreciable impact on the safety and/or well-being of the victim.

163. Further, Nguyen defines "victim" so as to encompass all who would provide their contact information. (*See,* Nguyen, 3:7-11.) Thus, it would have been obvious to a person of ordinary skill in the art that other interested third parties (*e.g.*, family members) would be suitable candidates for receiving inmate status notifications, either simply because they desire to be updated about their relative's status, or because their safety and well-being may also be impacted depending on their relative's status. Upon being informed of a change in status of a particular inmate, the control station "automatically calls and informs the victim of the change." (Nguyen, 2:3-5.) Therefore, Nguyen discloses "*notifying said third party*

of transfer of the inmate from one facility of the multiple facilities to another facility of the multiple facilities."

164. In addition, Hodge discloses "establishing another inmate account associated with said third party responsive to transferring the inmate to the other facility." Although Hodge discloses that "[a] user must have a system account established in order to make telephone calls from a specific facility" (Hodge, 42:14-15), Hodge states that "[w]hen an inmate is transferred from one facility to another, **only** the inmate's account information, COS, and telephone lists are transferred to that facility." (Hodge, 42:17-20 (emphasis added).) As discussed above in claim 2, in Hodge, an inmate's family (third party) may "add funds" and "thereby control the call volume allowed to the inmate." (Hodge, 2:39-46.) The transferred account information would include information associated with the family (third party). Thus, a person of ordinary skill in the art would recognize from Hodge that a new account will need to be made at the new facility, presumably based on the transferred account information.

IX. Conclusion

165. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within

the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this 15th day of May 2017 in Holmdel, NJ.

Respectfully submitted

L J. Forys

Leonard J. Forys