

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL

**OTD Briefing on:
Voice over IP (VoIP)**

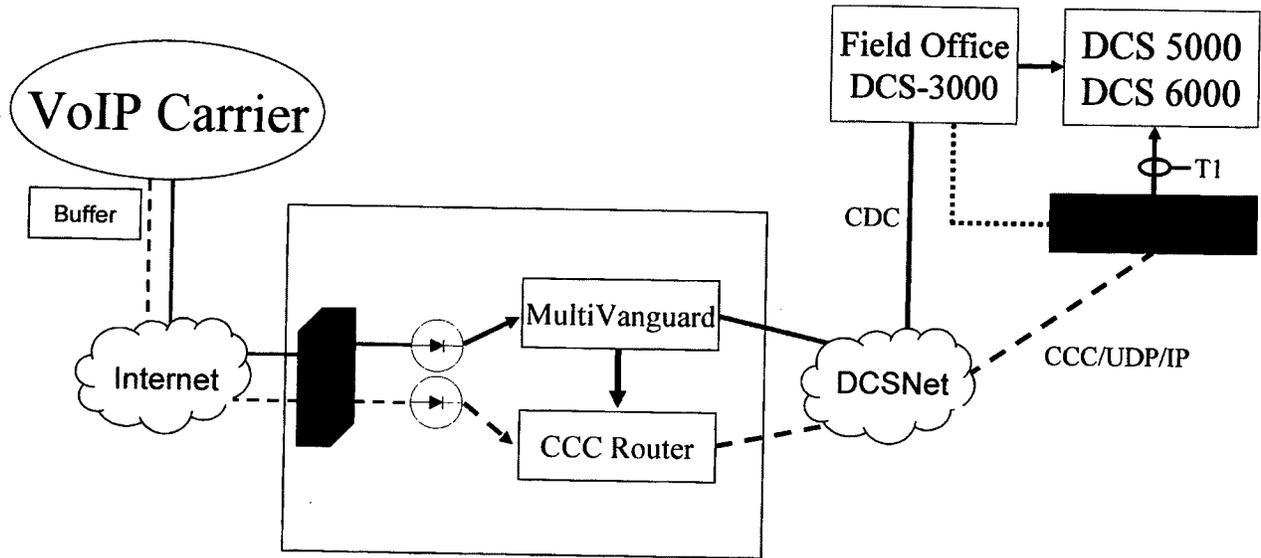


Director's Advisory Board Meeting





VoIP





Voice over IP (VoIP)



- What is it?
 - Technology used to transmit voice conversations over data networks
- Importance
 - Extremely cost effective for providers
 - Will eventually replace traditional PSTN telecommunications
- Types of VoIP
 - Carrier Grade – Quality ensured
 - Peer-to-Peer – No intermediary provider

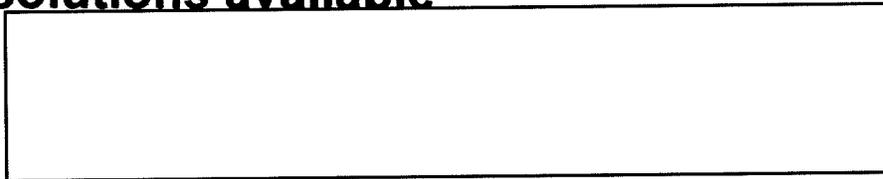


VoIP



Managed Carrier VoIP Experience

- **Some VoIP carriers have already embraced CALEA and have intercept solutions available**



b2
b7E

- **The solutions deployed by these carriers have forced FBI/OTD to develop a new access model:**



over the

b2
b7E

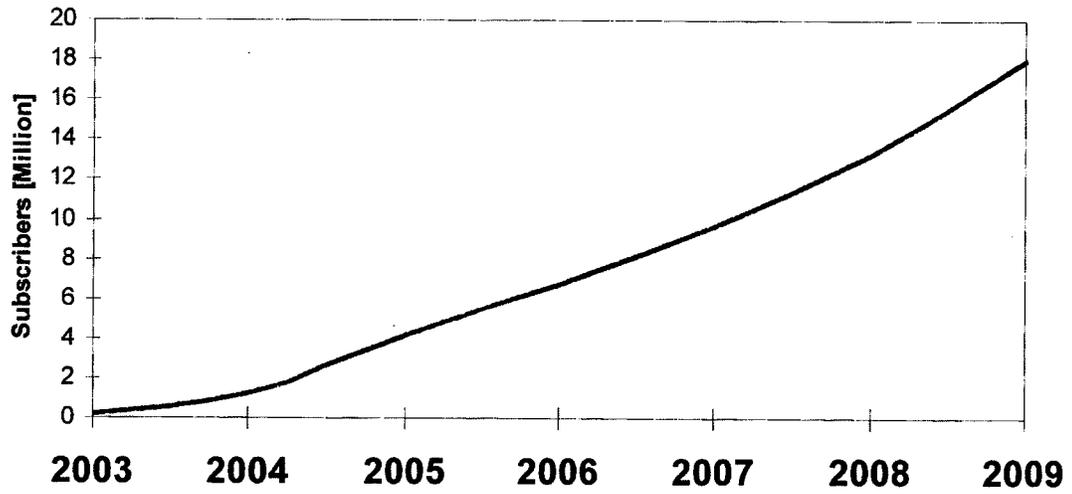
Internet



VoIP



Managed U.S. Residential VoIP Subscribers



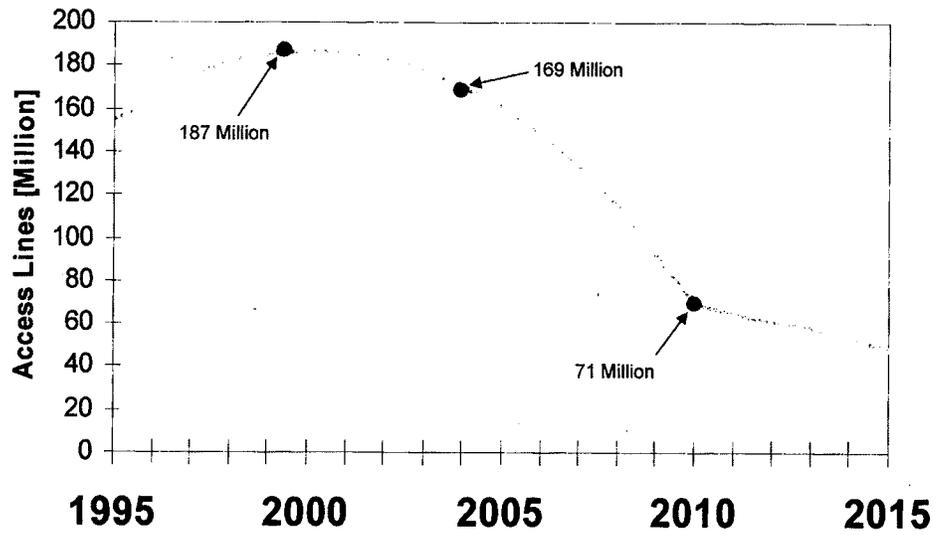
Source: Telecommunications Industry Association



VoIP



ILEC Narrowband Access Lines



Source: Technology Futures, Inc.



VoIP



Two Categories of VoIP

- **Managed**

- **“Pay for” services**

- AT&T
 - Verizon
 - Vonage

- **Unmanaged**

- **“Peer-to-Peer” services**

- Skype
 - Paltalk
 - Google Talk



VoIP

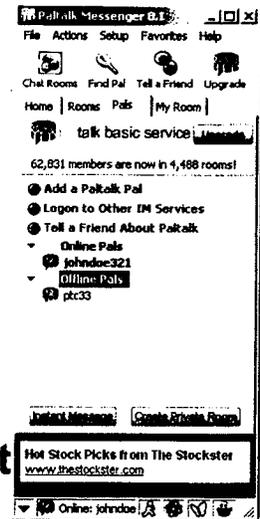


Unmanaged Software VoIP Technologies

- **Computer Internet Applications**

- Yahoo! Messenger, MSN Messenger, Paltalk, AOL Instant Messenger and Google Talk all utilize VoIP to allow computer-to-computer conversations

- **Utilizes free software installed on a computer and a microphone to transmit voice to another PC**



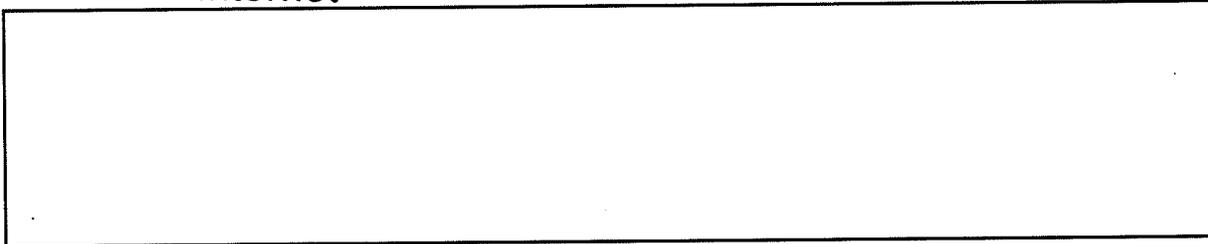


Technical Challenges



Encryption Example

- A company wants inexpensive telephone service between offices in NY and LA
- They set up a secure VPN connecting the offices over the Internet



b2
b7E

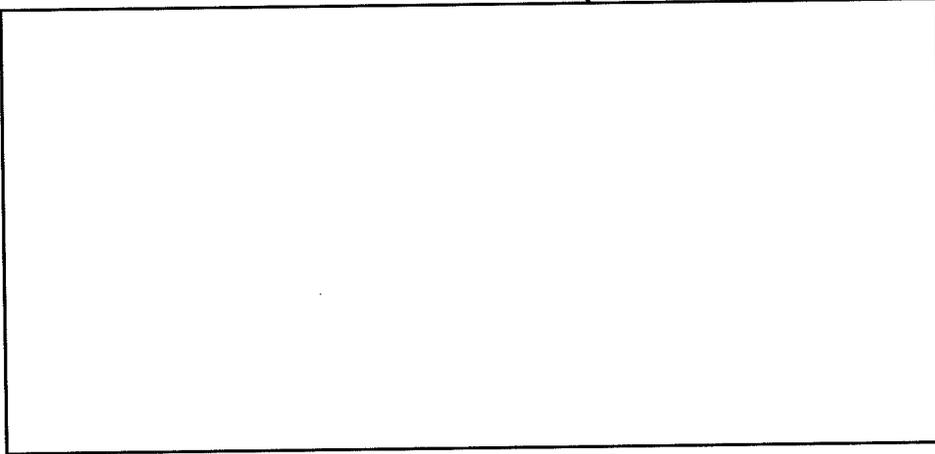


VoIP



Mobility of VoIP devices

- VoIP interface devices are portable



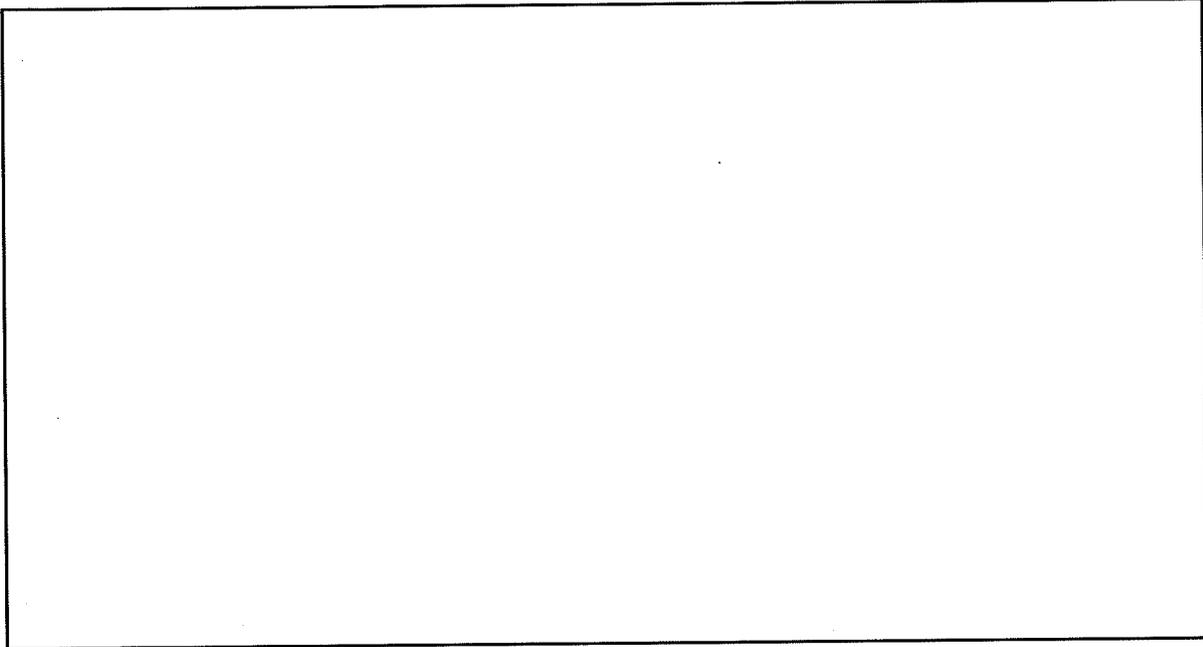
b2
b7E



Technical Challenges



Mobility Example



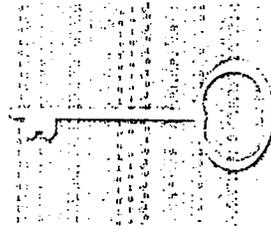
b2
b7E



Technical Challenges



Encryption



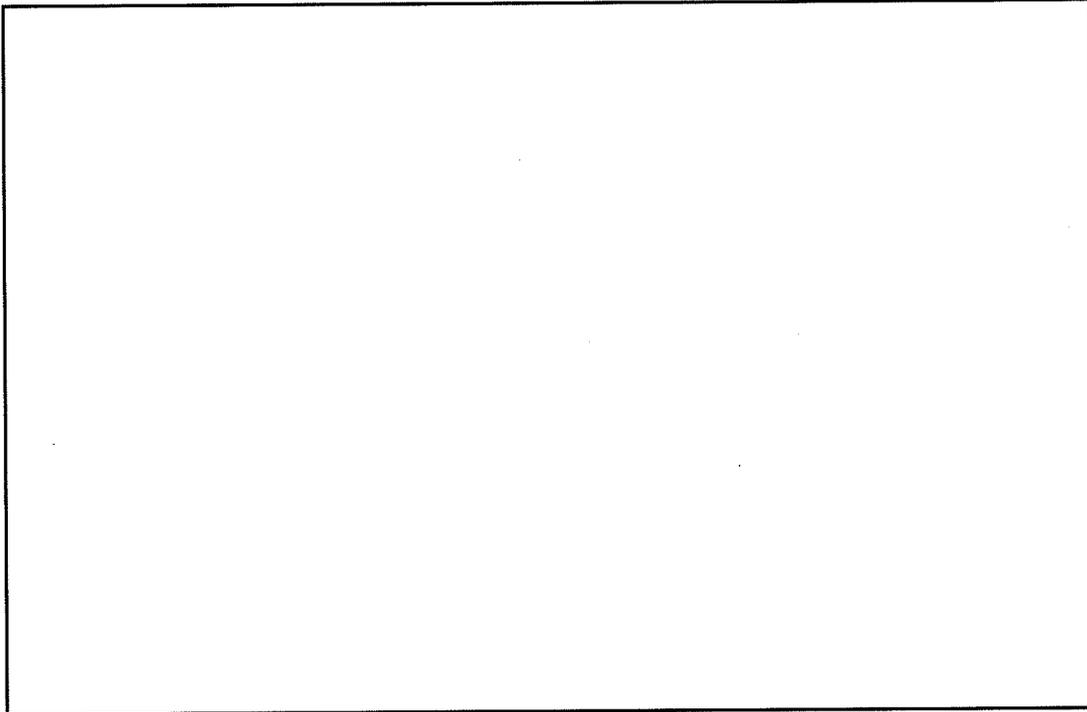
- VPN connection between offices creates a secure private telephone system
- VoIP command messages can be easily encrypted
- Skype, Gizmo and other VoIP service providers offer secure encrypted voice service for a global market



VoIP



VoIP Challenges

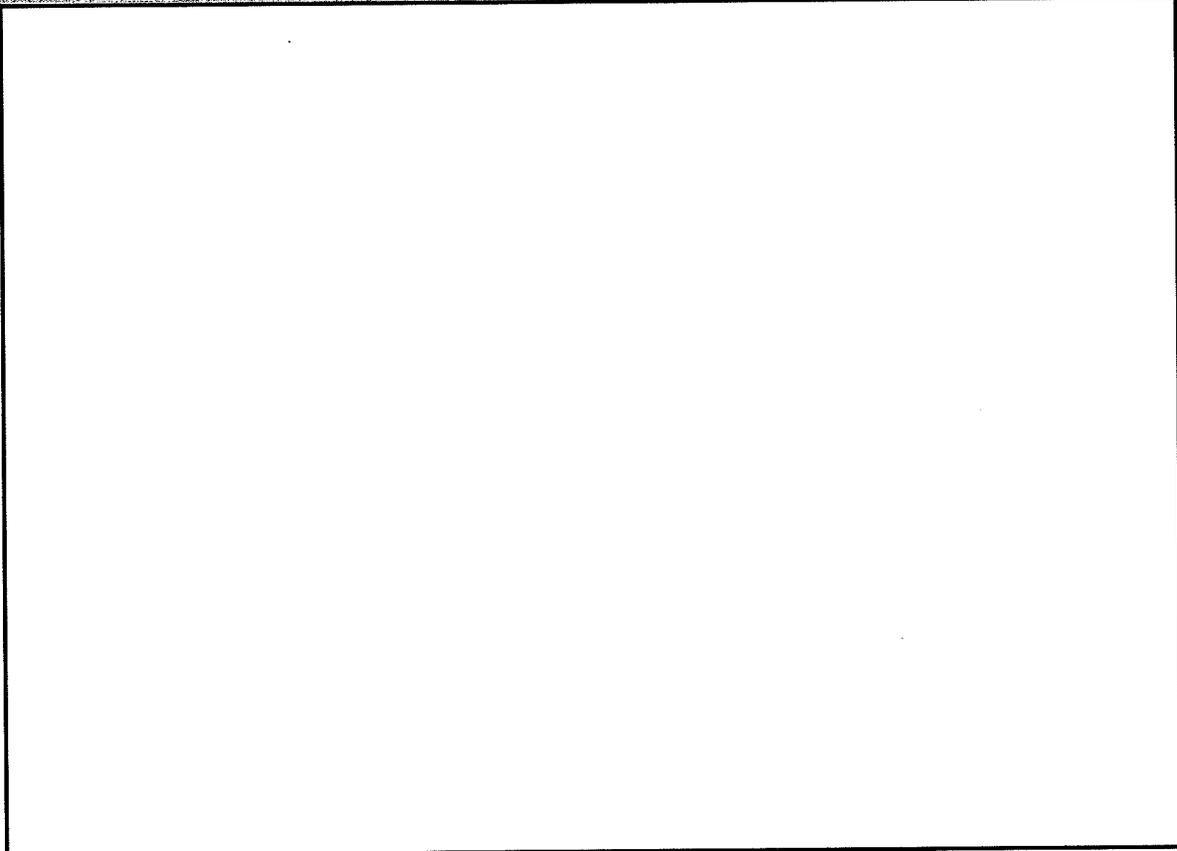


b2
b7E



VOICE OVER IP





b2
b7E

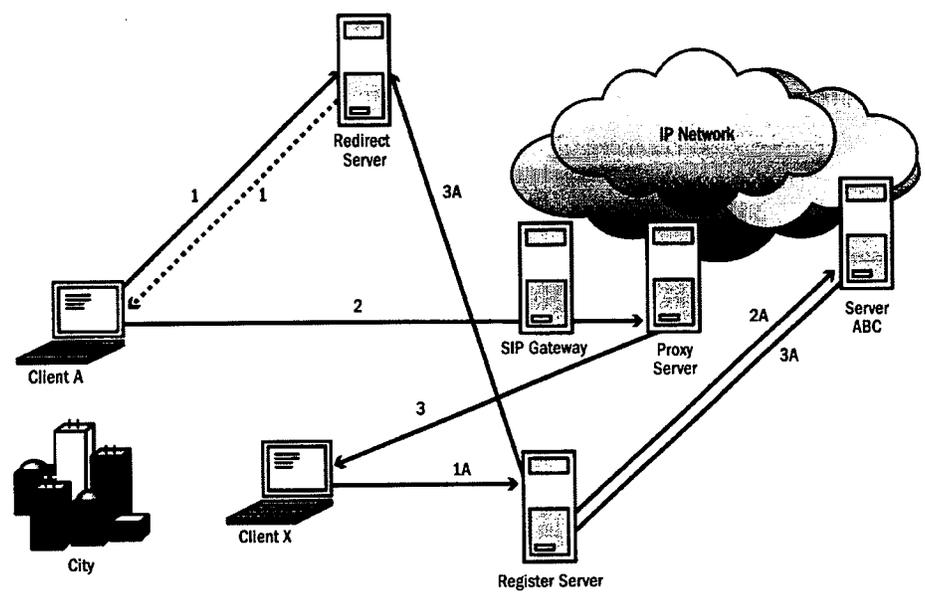


Figure 5.1. SIP Network Diagram

5. A meta buddy is an individual within a buddy list that has multiple service provider access points. Creating a meta buddy list involves locating all the service providers that the individual is registered to utilize.

B. IP MULTIMEDIA SUBSYSTEMS (IMS)

INTERNET TELEPHONY

INTRODUCTION

IP Multimedia Subsystem (IMS) Internet telephony—sometimes referred to as Multimedia Domain (MMD) telephony—is a 3GPP,¹ 3GPP2,² and Parlay Forum³ effort to define an all-IP-based wireless network (see Figure 8.1), in contrast to disparate legacy voice, data, and control networks and their operations, administration, maintenance and provisioning support infrastructures. The important advantage of IMS is that it is independent of the underlying access technology, such as the 3G Radio Controller (RNC). Most service providers are adopting IMS as the de facto convergence model for fixed, mobile, and enterprise telephony. IMS includes support for management of user registration and mobility. The major IMS architectural components and functionality of IMS are well defined by standards and already are under product development by many of the major telecommunications equipment suppliers.

Internet telephony and multimedia communications services, supported by companies such as Microsoft, Yahoo!, AOL, and Skype, have devised proprietary architectures to compete with incumbent service providers. The IMS architecture enables incumbent service providers to avoid becoming low-margin “bit pipe” providers and to leverage their existing access networks and customer bases. IMS is optimized for the Internet, with no

constraints from legacy telephone systems. It enables service providers to focus on user services rather than simply on transport. Moreover, under IMS service providers are not hindered by past commitments to Time Division Multiplex (TDM) networks.

IMS has no switches; there are no circuits to switch. Telephony is just another Internet application, similar to e-mail, file transfer, video streaming, and many others. The software technology comes from the IT industry—for example, standard operating systems, Java, and Session Initiation Protocol (SIP). SIP messages are structured in plain English text. They carry information about which codec to use, as well as parameters for the Real-Time Transport Protocol (RTP) connection.

The development cycles for IMS are short, and the platform for innovation is maximized. Because telephony is just another application, anyone can provide telephony services—even an entity that is not an access provider. The number of players will increase dramatically, as evidenced by the entry of Microsoft (MSN), Yahoo!, AOL, AT&T CallVantage, Skype, and Vonage, all of which already are active in this market.

Gateways connect the two worlds of TDM and IP. IMS is remarkably independent of the past and will be able to provide the platform for multimedia services for the next ten years, including new technologies, service concepts, players, and customer demands.

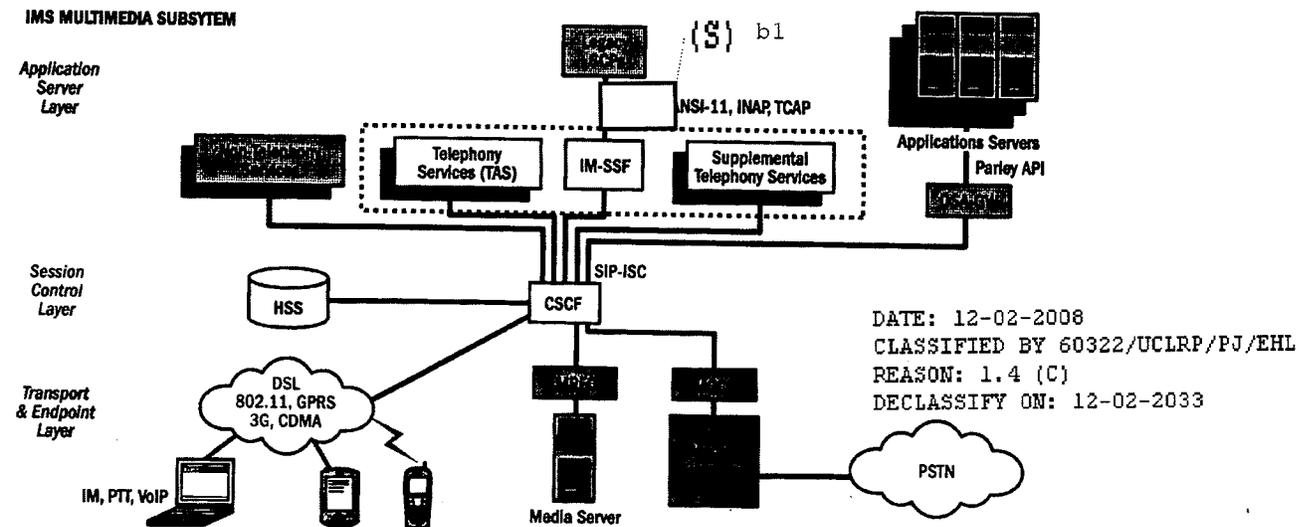


Figure 8.1. IMS Multimedia Subsystem

DATE: 12-02-2008
 CLASSIFIED BY 60322/UCLRP/PJ/EHL
 REASON: 1.4 (C)
 DECLASSIFY ON: 12-02-2033

1. 3GPP Third Generation Partnership Project - European Telecommunications Standards Institute (ETSI).
 2. 3GPP Third Generation Partnership Project2 - Developing the next generation of cdma2000 wireless communications.
 3. The Parlay Group aims to intimately link IT applications with the capabilities of the telecommunications world by specifying and promoting Application Programming Interfaces (API) that are secure, easy to use, rich in functionality, and based on open standards (<http://www.parlay.org/>).

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED EXCEPT
 WHERE SHOWN OTHERWISE

In Internet telephony, a constant identifier is the user's symbolic name (e.g., smith@service-provider.com), although the user's IP address will change. The required lookup, commonly known as ENUM, can be either centralized or decentralized. Microsoft MSN, Yahoo, and AOL telephony use a centralized lookup; Skype, through its free software downloads, uses a decentralized directory. Skype uses the FastTrack's well-known peer-to-peer file sharing application, KaZaA. Each PC stores and updates a part of the worldwide directory, using a Distributed Hash Table (DHT) algorithm. Updates and searches are done by cooperating individuals, and not by a single service provider function.

IMS provides a framework for communications of any type, anywhere, anytime—the ultimate goal of users and service providers alike. Concepts such as bandwidth-on-demand (based on the application, and only during the application session) and real-time, secure, multimedia, delivered via wireless broadband access, are designed into the standard, allowing individual equipment vendors and applications service providers to plug-and-play, thereby expanding the provider scope and assuring the greatest selection of value-added services.

b2
b7E



The IMS architecture is designed to support multivendor deployments. Layer functionality and protocols are well-defined. Many vendors will be offering components of the overall system, providing specific functionality or applications without knowledge or control of the system as a whole. The systems integrator and network service provider will be responsible for compliance with assistance to Communications for Law Enforcement Act (CALEA). Individual "box" manufacturers may have certain responsibilities as well, particularly if specified by the integrator.

IMS ARCHITECTURAL OVERVIEW

The IMS architecture comprises 12 major components (see Table 8.1); the IMS standard specifies the definition and functionality of each component. The ETR Bulletin Volume 2, Issue 2 (July 2005) highlighted the role of individual subsystems that assist in meeting overall CALEA capabilities, citing the Lucent Technologies IMS CALEA capability.

The IMS service architecture is a unified architecture that supports a range of services enabled by the session set-up capability provided by SIP. IMS can support multiple application servers offering traditional telephony as well as nontelephony services (e.g., Instant Messaging (IM), Push-to-Talk (PTT), video

telephony, and video). The service architecture is a collection of logical functions, divided into three layers (see Figure 8.1).

- Transport and Endpoint Layer
- Session Control Layer
- Application Service Layer

TRANSPORT AND ENDPOINT LAYER

The transport and endpoint layer initiates and terminates SIP signaling to establish (and set up) sessions and provide bearer services, such as conversion of voice from analog/digital to IP packets using RTP. The media gateways convert Voice over IP (VoIP) bearer streams to the PSTN TDM format within this layer. The media server also provides related media services, such as user conferencing, service announcements, collection of in-band signaling tones, speech recognition, speech synthesis, and other services.

Media server resources are shared across all applications. Any application that requires service calls on a common server to meet its need. Applications include voicemail, advanced 800 service, and interactive Voice eXtensible Markup Language (VXML) services, among others. The media server also supports nontelephony functions such as replicating media to provide for PTT service.

SESSION CONTROL LAYER

This layer includes the Call Session Control Function (CSCF), which provides registration of endpoints and routing of SIP signaling messages to the appropriate applications server. The CSCF plays a critical role in intercepting call identification information for law enforcement. The CSCF interacts with the transport and endpoint layer to guarantee QoS across all services. The session control layer includes the Home Subscriber Server (HSS) database, which maintains the unique service profile for each authorized user. This user service profile includes all user service information and preferences in a central location which provides critical information for law enforcement. This database includes users' current registration information (IP address), roaming information, telephony services (call forwarding information and call acceptance), IM information (buddy lists), and voice mailbox options. Centralized information supports and simplifies administration of user data and provides consistent views of user profiles across applications, regardless of service provider. This function enables creation of unified personal directories, multient presence information, and blended services.

APPLICATION SERVICE LAYER

The application service layer incorporates application servers that provide the user service logic. The IMS architecture and SIP signaling are designed to support a variety of telephony and nontelephony applications servers, including IP multimedia services.⁴

4. IETF RFC 3428, "Session Initiation Protocol Extensions for Instant Messaging"

1. Access Gateway (AG): Provides an interface between the IP-based network and the radio access network. (MOBILE)
2. Access Network (AN): Radio component of the network. (MOBILE)
3. Breakout Gateway Control Function (BGCF): Controls all resources allocated to the IP session. (NETWORK CONTROL)
4. Call Session Control Function (CSCF): Provides control and routing function for IP sessions. (NETWORK CONTROL)
5. Foreign Agent (FA): Advertises itself to mobile stations in the serving area. Provides registration information to Home Agent. Forwards packets from mobile to Home Agent. (MOBILE)
6. Home Agent (HA): Tracks all current FAs serving the mobile. Forwards packets to the current FA. (MOBILE)
7. IP network. Contains Authentication, Authorization and Accounting (AAA) function and other required service databases; can be IPv4 or IPv6 (NETWORK)
8. Media Gateway (MGW): Provides an interface for bearer traffic to/from the public switched telephone network (PSTN) and IP networks. (PSTN TRAFFIC _ LEGACY)
9. Media Gateway Control Function (MGCF): Provides signaling interoperability between IP and PSTN domains (e.g., SIP to Integrated Services Digital Network User Part (ISUP), ISUP to SIP) (PSTN SIGNALING _ LEGACY)
10. Policy Decision Function (PDF): Assigns resources according to application demand and required Quality of Service (QoS); unlike TDM networks, IP networks assign network bandwidth and resources in real time (NETWORK CONTROL)
11. Position Determination Entity (PDE): Although a growing number of mobiles incorporate Global Positioning System (GPS), the PDE can provide assistance in determining geolocation by using network measurements and complex algorithms (NETWORK SERVICES)
12. SIP Application Server (SAS): A platform for SIP application development and operation (IP CALL SETUP)

triggers, including user call triggers. If a trigger is observed, the TAS suspends call progress and determines, on the basis of the subscriber's service profile, what additional application services are to be applied at that point in the call. If called for, the TAS formats an SIP IP Multimedia Service Control (ISC) message and passes call control to the appropriate application server. The TAS supports legacy AIN functionality as well as new SIP-based applications servers.

A single IMS supports multiple TASs that provide specific features to endpoints, based on authorized services (user profile). For example, one TAS can support IP Business Centrex features (i.e., private dialing plans, shared directory numbers, multiple call appearances, Automatic Call Distribution (ACD) and attendant services), and another could support Private Branch Exchange (PBX) and provide for advanced Virtual Private Network (VPN) services. Multiple application servers can use SIP-I signaling to complete calls between different classes of users.

IP Multimedia - Services Switching Function (IM-SSF): The IM-SSF provides the interworking of SIP messages to corresponding

American National Standards Institute-41 (ANSI-41), Intelligent Network Application Protocol (INAP), or Transaction Capabilities Application Part (TCAP) messages. This interworking is required to allow IP phones supported by IMS to access services such as calling name service, 800 services, Local Number Portability (LNP) services, and one-number services ("find-me-follow-me" services).

b1

Supplemental Telephony Application Servers: The application server layer also supports standalone independent servers that provide supplemental telephony services at the start, middle, or end of a call, via AIN-like triggers (user-to-network signals). Such services include "click to dial," "click to transfer," "click to conference," voicemail services, Independent Voice Recognition (IVR) services, VoIP VPN services, prepaid billing, and inbound/outbound call blocking services.

Nontelephony Application Servers: The application layer also can support SIP based application servers that operate outside the telephony call model. These application servers can interwork with user endpoint clients to provide services such as IM, PTT, and presence-enabled services. Implementation of nontelephony SIP-based services in a common IMS architecture permits interworking of telephony and nontelephony services to create new, blended communication features and capabilities. An example is a "click to contact" buddy list that displays end user presence and availability information, which provides a point-and-click interface across multiple communication services (telephone, IM, and PTT). Another example is the use of a single prepaid account for telephone and nontelephony services.

Open Service Access - Gateway (OSA-GW): The IMS architecture has a flexible design which allows services to be added into the VoIP networks by interacting with legacy applications or by

Telephony Application Server (TAS): The TAS is a back-to-back SIP user agent that maintains the call state. The TAS contains the service logic that provides basic call processing services, including digit analysis, routing, call setup, call waiting, call forwarding, conference bridging, and other well-known telephone features. The logic required to invoke the media server to support appropriate call process tones and announcements resides in the TAS. If calls originate or terminate on the PSTN, the TAS provides SIP signaling to the Media Control Gateway Function (MCGF) to instruct the gateway to convert the PSTN TDM voice bitstream to an IP RTP stream and direct it to the IP address of the corresponding IP phone.

integrating SIP-based applications with existing legacy systems and specific applications. IMS supports service providers, permitting their customers to develop and implement services that leverage VoIP network resources. For example, if an enterprise wanted to voice-enable a back-office operation to automatically initiate a call if an order was rejected because of missing shipping information, this function could be triggered by a Personal Digital Assistant (PDA)-like scanning device that recognizes information is missing and communicates the trigger function to the applications server.

the call. The P-CSCF is the entry point of the system to send its SIP messages with the signaling gateway. A proxy CSCF or P-CSCF as this entry point. All phones have the address of the P-CSCF. Messages are then forwarded to the home interrogating CSCF (I-CSCF). The P-CSCF serves as the visiting Session Control Function Server, and the I-CSCF is the home Session Control Function Server.

Legacy Network Interaction: If the call terminates on a legacy number, the S-CSCF detects this and interfaces with the BGCF. The MGCF is selected and performs the translation between SIP messages and the ISUP Signaling System 7 (SS7) message. It also controls the MGW, which performs the translation between the Internet voice flow (RTP) and the legacy PCM voice flow.

MIGRATION TO IMS

The SIP⁵ signaling, RTP,⁶ and IMS architecture were developed to rapidly move beyond broadband voice and data services and into the realm of advanced broadband multimedia services such as broadcast television using multicast IP video streams, video-on-demand, video surveillance, video telephony, videoconferencing, virtual classrooms, video e-mail, and similar applications yet to be invented. All of these services and more can be introduced by equipping the network with additional multimedia application servers and supporting endpoint devices. (Figure 8.2 highlights standardized architectural support for traditional non-SIP telephony.)

As new broadband multimedia services become prevalent, bandwidth management will be required to provide for QoS beyond the basics available today. Monitoring and control of available bandwidth will affect the number of active, real-time communications sessions. Endpoints will send their SIP requests

(S)

b1

In many cases, IT programmers are not familiar with complex telephony signaling protocols such as SIP, ANSI41, Integrated Services Digital Network (ISDN), and [redacted]. To provide a simple Applications Program Interface (API) the Parlay Forum, working with 3GPP and ETSI, has defined an API for telephony networks. This interface between SIP and the API is provided in the OSA-GW, which is part of the application service layer. The OSA-GW allows enterprise-based API applications to access presence and call-state information, set up and take down sessions, and manage and change call legs. The enterprise applications servers can register with the network and manage access to network resources. This capability introduces enhanced third-party applications programming to the communications path.

IMS CALL FLOW

IMS is based on the Internet, which carries packets over fixed or mobile networks. IMS implements roaming and enables users to take their phones anywhere as long as they identify themselves via a login and password process. The architecture is not limited to Internet telephony. It is a platform for a wide range of new communications and information services.

IP Telephony: When a phone is connected to the network, it sends an SIP message to register with the HSS, which stores the directory for its domain. This function manages the association between the symbolic name and the IP address. To initiate a call, the user SIP phone sends an INVITE message via the Serving - Call Session Control Function (S-CSCF), where the address is resolved. The S-CSCF determines which application to activate—e-mail, voice, or video—and, for law enforcement, whether interception is required. The S-CSCF then forwards the INVITE message to the appropriate IP address. The S-CSCF is not a switch. It is a serving function that is integral to the application of lawful interception. It performs the following functions:

1. Identifies the caller's service privileges and S-CSCF of called party
2. Replaces the symbolic name of called party with IP address
3. As required, the SIP message is forwarded to an applications server and performs an operation based on the applications server directions.

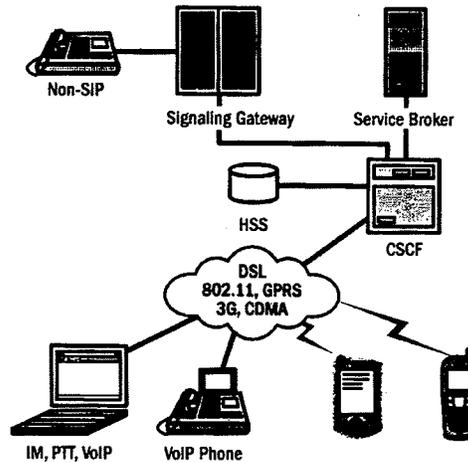


Figure 8.2. Location Service Infrastructure Example

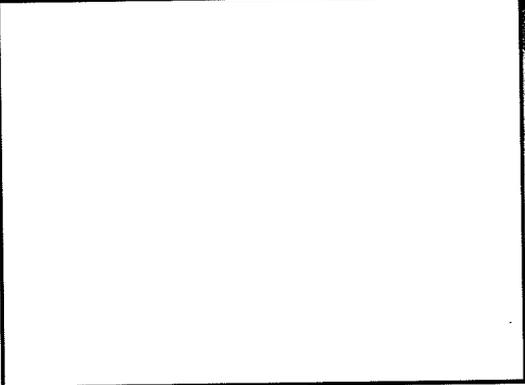
5. SIP is used to set up calls between hosts, starting with the INVITE message, with parameters for the RTP connection. The answer is a RINGING message, followed by an off-hook, OK message. Following the ACK message, a RTP connection is established. SIP also can be used for instant messaging.

6. RTP transports voice and video. The sender uses a codec to encode the flow in a format such as G711, MP3, Advanced Video Coding (AAC), or Motion Picture Experts Group (MPEG).

... a common... the... with... transport and endpoint layers of the network to assess current traffic levels and can deny requests for additional sessions of applications that request additional bandwidth.

3.

Extensions of the IMS architecture to support new services are on the horizon. Today only a fraction of the endpoints support SIP signaling. IP-PBX typically uses H.323 signaling. Integrated Access Devices (IAD) use Media Gateway Control Protocol (MGCP) to provide VoIP over Digital Subscriber Lines (DSL). Supporting these numerous endpoints in an IMS network will require supporting non-SIP signaling (e.g., non-SIP to SIP). 3GPP proposes the introduction of new border signaling gateways to provide for this interworking. The architecture clearly is flexible enough to provide for this specific functionality, enabling a linkage from present to future. IMS is well suited to support specific interworking and brokering services, enabling blended features to offer new services to users without major changes in the basic platform. The result will be rapid introduction of new, value-added services that are proprietary to a specific service provider yet are fully compatible with the over all "public" network. The concept entails a service broker or interaction manager element that will share application state and communication status information between applications, allowing for smooth introduction of new capabilities.



b2
b7E

CONCLUSION

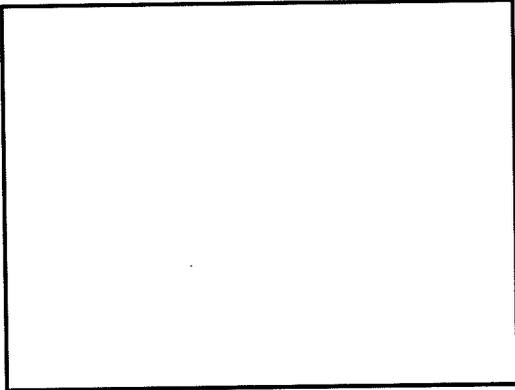
IMS is the future architecture for internet multimedia telephony. It provides an ideal standardized architecture that will allow service providers—large or small, incumbent or start up—to introduce a plethora of broadband multimedia services that require bandwidth on demand and rely heavily on a broad spectrum of third-party application developers and independent applications service providers. In many cases, applications will be proprietary to the provider, and complete knowledge of the communication will not reside at a single point. Furthermore, as with all IP network applications, the server need not be centralized or in a defined geographic territory.

IMS involves no circuits, or circuit emulation, and there are no switches. It is not constrained by legacy telephony and thus will take advantage of advances in Internet technology.

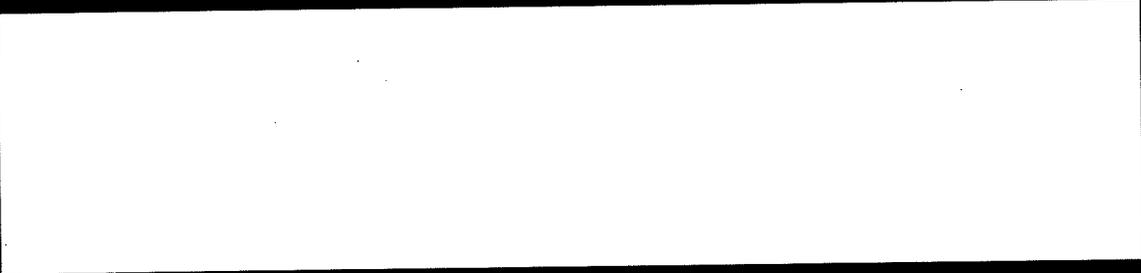
IMPLICATIONS FOR LAW ENFORCEMENT

There are three significant implications for law enforcement:

- 1.
- 2.



IMS adds functions in the network (i.e., between the hosts) to make the services easier to use or to add functionality to the services. It is easy to add a new application, in the form of a SIP message processing function for each new service created. Network operators propose to use IMS in place of proprietary solutions proposed by Microsoft, Yahoo!, Skype, and AOL.



LATEST NEWS

SEPTEMBER 2005 - Lucent Technologies Bell Labs announced the first reported transmissions of 100 Gigabit per second (Gbps) Ethernet-over-optical.

Ethernet signals are transported over 10Gbps and, occasionally, over 40Gbps SONET connections. Bell Labs effort is aimed at producing 100Gbps Ethernet-over-optical transmission.

The Bell Labs research team was able to deliver a 107 Gbps optical data stream, representing 100 Gbps of data transmission plus a standard 7 percent overhead for error correction, using the following two technological approaches:

- **Duobinary Signaling:** This technique uses three electrical signal levels, — positive, negative and zero — to represent a binary signal for communications transmission. Duobinary signals require less bandwidth than traditional NRZ (non-return to zero) signals. The application of this bandwidth-compressing format enabled the creation of an optical 107-Gbps serial data stream using a commercially available optical modulator (rated for 40 Gbps).
- **Single-Chip Optical Equalizer:** Integrated optical equalizers invented by Bell Labs researchers two years ago, can compensate for transmission impairments and also for the limited modulator bandwidth in a commercially available NRZ system. NRZ is the least complex optical data format to generate. In order to demonstrate an optical 107-Gbps NRZ signal, Bell Labs designed a single chip optical equalizer that compensated for almost all inter-symbol interference arising from modulator bandwidth limitations in an optical 107 Gbps NRZ electronic time division multiplexing (ETDM) transmitter. As with the Duobinary approach, Bell Labs researchers used a commercially available 40-Gbps optical modulator in combination with the optical equalizer to generate a 107-Gbps optical NRZ data stream.

DECEMBER 2005 - San Francisco advanced their Wireless TechConnect program, whose goal is to provide free wireless service to everyone in the city and county, by releasing a Request for Proposal (RFP) with proposals due in February 2006. The program is geared towards providing free WiFi access to the Internet, affordable hardware, training, and support to low income and disadvantaged residents. The RFP calls for 95% of outdoor areas and 90% of indoor areas in San Francisco city and county to be covered by 802.11b and/or 802.11g service for a maximum term of 18 years, and WiFi security to be supported including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), and the Advanced Encryption Standard (AES) algorithm.

DECEMBER 2005 - Nortel Networks and Option N.V. completed the industry's first successful demonstration of live HSDPA data card calls reaching a wireless transmission rate of 3.6Mbps - faster than the majority of current broadband connections. The test calls were

carried out on commercial HSDPA network equipment at Nortel's research campus. The series of calls are the first data card calls to demonstrate downlink speed of 3.6 Mbps, at HSDPA category 6 using 16 Quadrature Amplitude Modulation (QAM) modulation. A laptop fitted with an Option 3.6 HSDPA datacard, based on QUALCOMM core MSM 6280 technology and commercial HSDPA network equipment from Nortel, were used to achieve the download speeds.

DECEMBER 2005 - Skype began offering the beta of the second version of their service, which now includes a free video calling service. The new video calling service allows parties to exchange real-time videos of themselves while conducting a phone call over the Internet. Video calls require the use of Skype-supported web cameras on user computers.

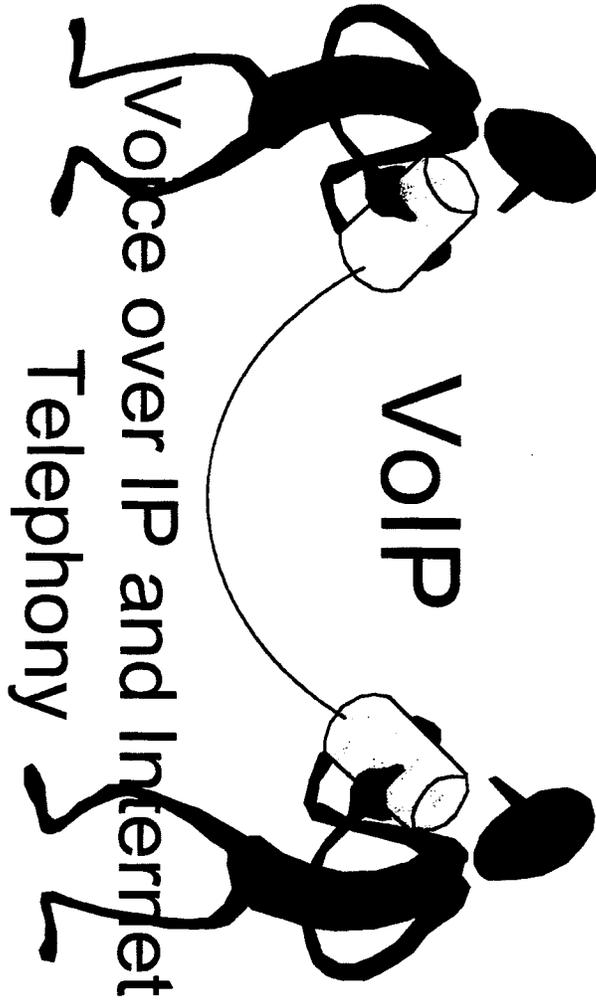
DECEMBER 2005 - IEEE formally ratified the 802.16e, Mobile Worldwide Interoperability for Microwave Access (Mobile WiMax). Mobile WiMax is a microwave-based standard for mobile, wireless, broadband connectivity that allows roaming among base stations and clients. The technology provides a range from a few hundred feet to a couple of miles depending on the how densely populated the area is and a maximum average speed of 20 Mbps per second as compared to WiFi's range of approximately 50 feet, but with a comparable average speed for data. Mobile WiMax products will become commercially available to residential customers to increase their broadband connectivity in 2006, and mobile devices are slated to hit the market in 2007.

JANUARY 2006 - Manufacturers are developing chips and products based upon the draft 802.11n standard that can deliver throughput data rates of up to 600 Mbps, drastically faster than 802.11a/b/g standards used by wireless LAN products today. The high-throughput wireless LAN standard 802.11n is approximately 40 times faster than 802.11b, and 10 times faster than 802.11 a and g standards. Actual throughput seen by users will be close to or better than what is seen on wireline networks. The drastic increase in throughput will enhance performance in data, voice, and video applications such as VoIP for users. An IEEE task force approved a draft specification for 802.11n in January 2006, with final approval of the specification expected to take approximately one year.

JANUARY 2006 - Netgear announced it will offer a mobile phone designed to work with Skype's VoIP service. The mobile phone looks like a standard cell phone and comes preloaded with Skype. To use the phone, subscribers enter a Skype username and password and must be able to access a WiFi connection, using either 802.11b or 802.11g. Once connected, users have access to their contact list and Skype directory. SkypeIn and SkypeOut services will also be supported, allowing users to make and receive calls to and from non-Skype users for an minimal fee. Netgear will announce the pricing and availability of the mobile Skype-enabled phones in the first quarter of 2006.

"Reference therein to any specific commercial product, process, or service by its trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof."

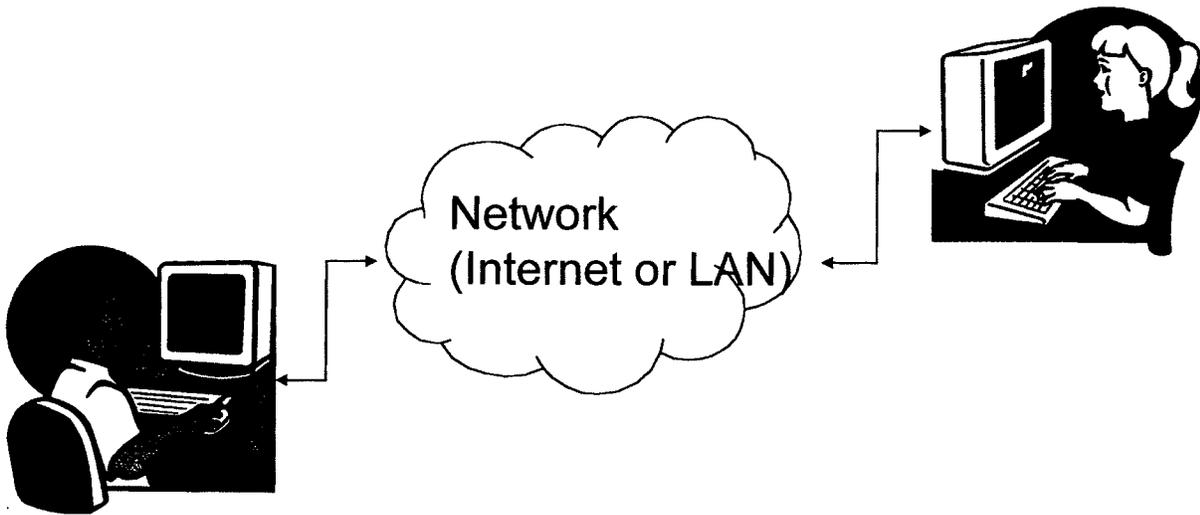
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL



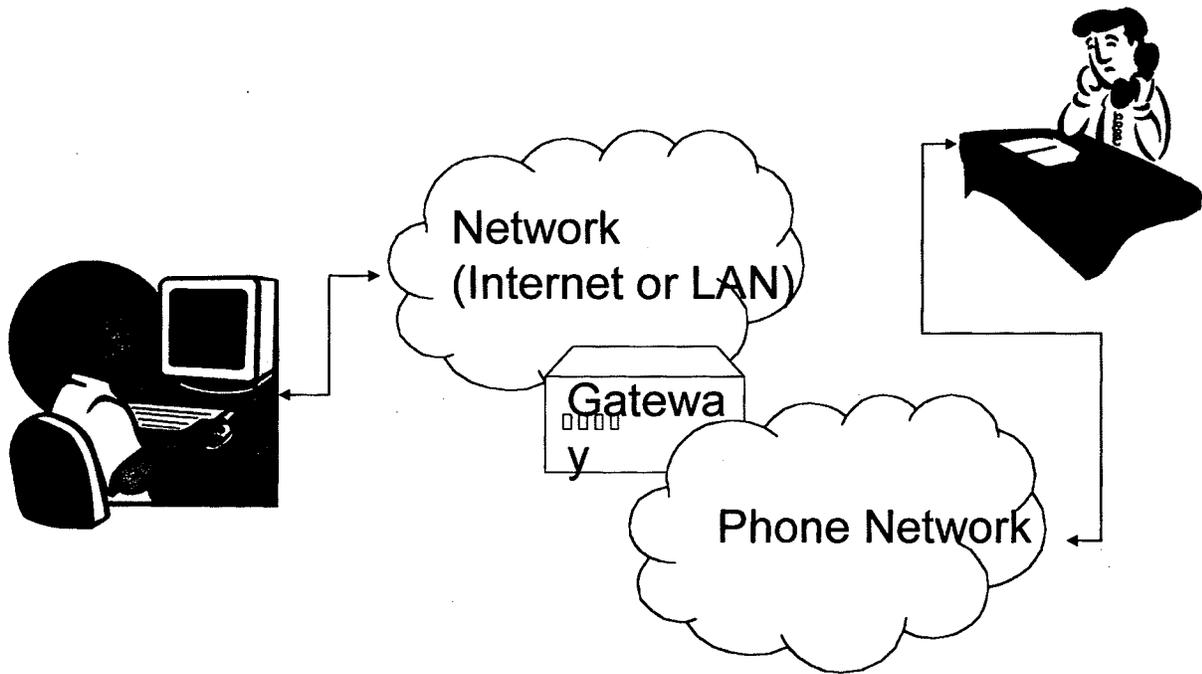
VoIP Overview

- Voice over Internet Protocol (VoIP)
- Utilizes computer networks for voice communication
- Can work over Internet or LAN (ex. office network)
- Both free and pay services exist
- Some have gateways to traditional telephone systems

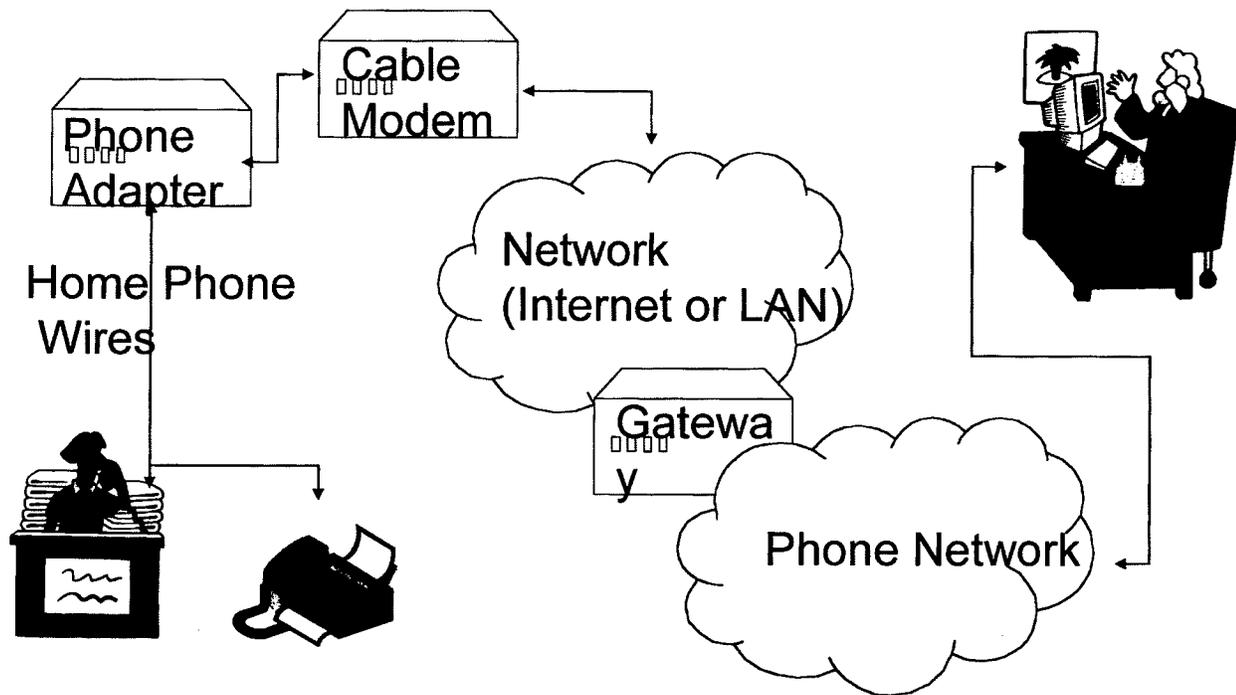
Peer to Peer



Computer VoIP to Telephone



Seamless VoIP to Telephone



Products and Services

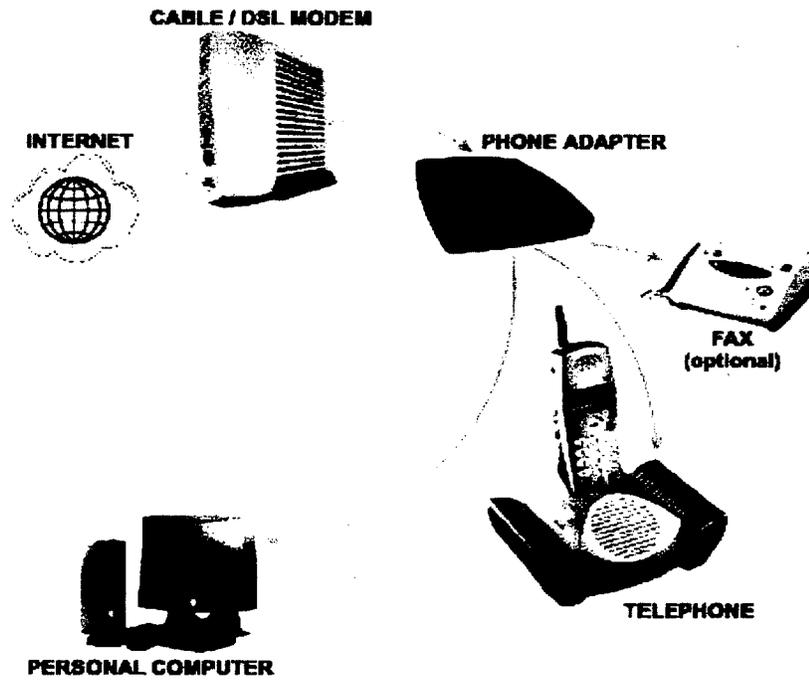
P2P Internet Phone

- Yahoo Chat
- AOL IM Chat
- Paltalk
- Skype
- FWD
- PGPfone

VoIP to Telephone

- Vonage
- 8x8
- Cable carriers
 - Cox
 - Comcast
 - TimeWarner Cable

Vonage



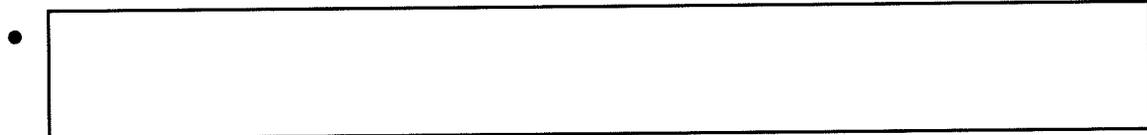
Vonage - \$15 gets you:

500 minutes local, regional, and long distance U.S. and Canadian calling.

Advanced Services: Area Code Selection, Online Account Management, Number Portability, Free Calls to Any Other Vonage Subscriber, Personalized Voicemail, Call Forwarding/Network Availability #, Call Waiting, Caller ID, Caller ID Block (*67), Repeat Dialing, Call Return (*69), Virtual Phone #, Call Transfer, Bandwidth Saver, Dialing 911, Softphone

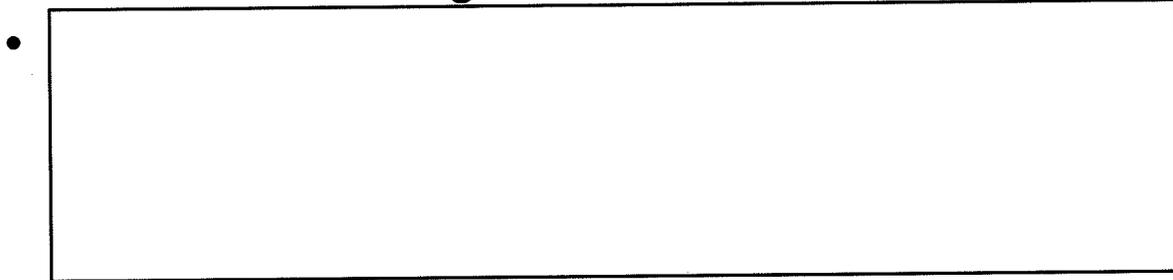
Current Events

- Most major cable providers are starting to roll out VoIP service.



b2
b7E

- Bills in Congress reserving regulation of all VoIP for federal govt.



Other Issues

- Wireless Internet phones

b2
b7E

- Encryption

- Use of

-

b6
b7C

[Redacted] (OTD) (CON)

From: [Redacted] (OTD) (FBI)
Sent: Friday, February 29, 2008 3:14 PM
To: [Redacted] (OTD) (FBI); [Redacted] (OTD) (FBI)
Cc: [Redacted] (OTD) (CON); [Redacted] (OTD) (CON); [Redacted]
Subject: FW: [Redacted] (OTD) (CON)

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

FYI

SSA [Redacted]
Operational Technology Division (OTD)
Remote Operations Unit (ROU)

b6
b7C

[Redacted] (cell)
[Redacted] (desk)
[Redacted] (fax)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL

From: [Redacted] (OTD) (FBI)
Sent: Friday, February 29, 2008 3:11 PM
To: [Redacted] (OTD) (FBI)
Subject: [Redacted]

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[Large Redacted Area]

b2
b7E

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL

b2
b7E

Software Documentation

January 2008

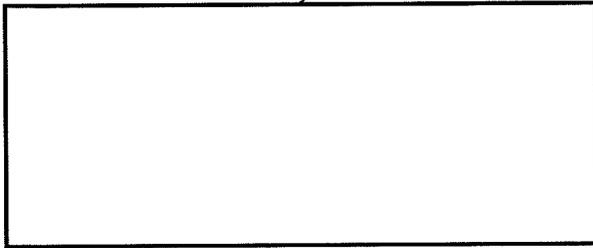
Rev. 3

Program Sensitive

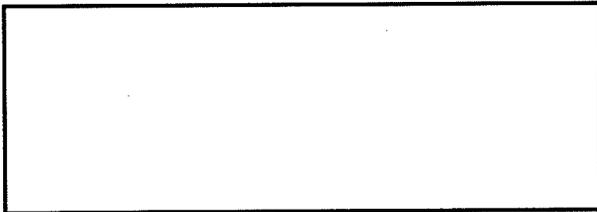
6/16/2008

2. Voice Over IP

—executive summary



Voice Over IP (VoIP) is a rapidly emerging technology with the potential to significantly change the communications environment. VoIP is being marketed by service providers as a consumer technology with the promise of inexpensive, worldwide telephone service with the same voice quality as existing circuit-switched technologies. There is an emerging consensus within the telecommunications industry that VoIP services and IP networks will effectively replace conventional circuit-switched telephone service in the next 5-10 years.



—technology

The traditional telephone network uses a circuit-switched design in which a phone conversation requires a dedicated circuit to be maintained while the conversation takes place. To accommodate the vast number of potential users, the circuit-switched network must provide dedicated circuits to handle the telephone traffic. During normal telephone conversations, a circuit must remain open and utilize its full capacity even though not all of each user's time is spent transferring data or talking. Typically, 50 percent of the circuit's capacity is wasted because at least one user in a conversation is listening or receiving data and not talking.

VoIP operates in an entirely different way. VoIP can be transmitted over the public Internet or service provider networks, offering customers phone service through various types of terminal equipment, such as telephones, computers, and PDAs (see Figure 2a). Further, with wireless VoIP service access, via cellular services and "WiFi hotspots," mobile VoIP services may be available to users anywhere in the world.

¹ Public Internet or private IP network

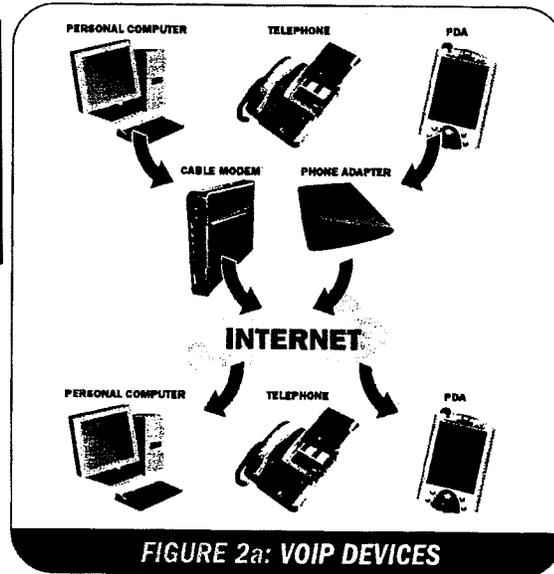


FIGURE 2a: VOIP DEVICES

b2
b7E

Packetized voice is sent through a network where dedicated circuits are not required. Voice data packets are routed through the network along with other data packets on an as-needed basis. This provides increased efficiency within the network and frees up network resources, as well as user resources sending and receiving information.

The technology converts voice signals to data streams that are transmitted over the public Internet. During a VoIP call, voice signals are sampled at the transmitting device and processed into digital data streams. The digital streams are placed, along with routing information, into data packets for transmission over the network¹. To effectively transmit the packets, both UDP/IP and TCP/IP protocols may be used to pass data packets over the Internet to the receiver. The data packets join the sea of data on the network and may be routed through multiple paths on their way to the receiver. No single point can be guaranteed to provide access to all the data packets necessary for reconstruction of the voice signal. At the receiver, the data packets are collected and reassembled into a data stream representing the original voice signal. The data stream is then processed to reconstruct the original analog voice signal, which is passed to the receiving device's speaker.

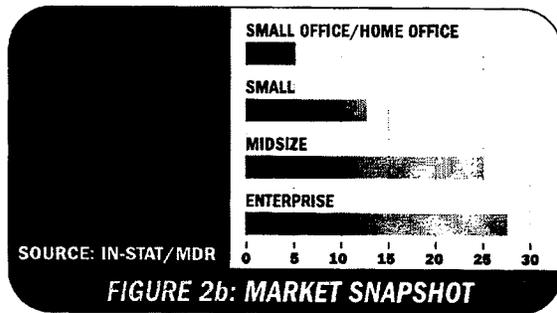
—service providers

Millions of consumers worldwide now use VoIP services, and these services are rapidly growing in popularity

driven by VoIP's ability to support inexpensive phone service. Although there is a modest fee for connection to the local Internet service, the phone call itself can be free of charge.

Currently, businesses are the biggest users of VoIP (see Figure 2b) because of their preference to use their existing data networks for telephony; however, residential VoIP is growing as households seek to fully utilize their broadband high-speed Internet service.

VoIP services are widely available from a number of sources. Traditional telecommunications service providers (AT&T), cable companies (Cox), and Internet service providers (AOL) all offer VoIP services at significantly reduced rates (compared to conventional circuit-telephone service). In addition, non-telecommunications-related entities offer software (and/or equipment) allowing free peer-to-peer Internet-based VoIP telephone service.

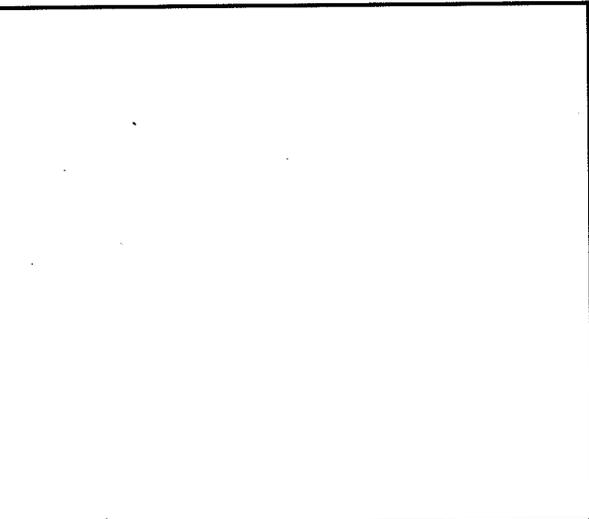


As the popularity of VoIP grows, the number of service providers will grow as well. In the early stages of VoIP's use and development, several small startup enterprises (SIPphone, Free World Dial-up, IPtel) offered services. Now larger companies are also entering the market. Vonage is an example of a major VoIP company, with more than 135,000 lines currently in service and 20,000 lines being added per month with over 5 million calls per week.² In addition to these VoIP companies, traditional telephone companies are entering the market. AT&T recently announced deployment of service in New Jersey and Texas, and it is anticipated that other major carriers will soon follow. (See page 5 AT&T article.)

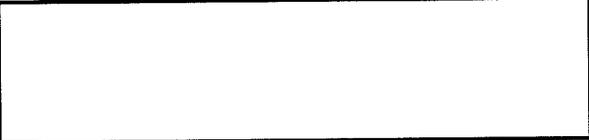
—application

VoIP is very simple to use. The user picks up the phone, listens for a dial tone, dials the number, and connects—the same process used with a circuit-switched phone. The difference is that the VoIP phone is connected to a broadband network access adapter.

In addition to using telephones attached to network adapters, users can place calls using VoIP directly from a computer, using either a conventional telephone or a microphone. For users who have existing Internet access, Internet telephony software provides free telephone calls anywhere in the world. Currently, however, PC-based Internet telephony does not offer the same quality of telephone service as does direct telephone connections. Users often experience signaling issues, quality of service issues, and delays. The user may also experience difficulties with firewalls and Network Address Translators (NAT). To provide a high-quality voice service, a broadband connection is required, either through a cable modem or high-speed services, such as DSL or a local area network.



—impacts on law enforcement

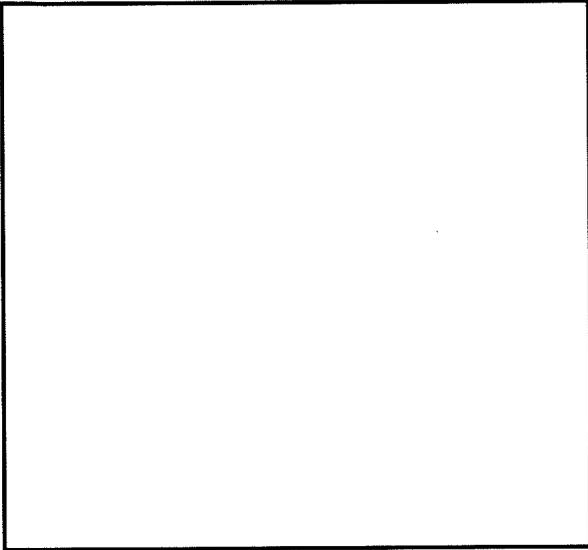


b2
b7E

—skype

Skype, a VoIP system built on a distributed peer-to-peer network, exemplifies the issues noted above. The system has no central server for data collection, and all packets, including Call Sent information, are sent through the network without the assistance of a central routing point. In addition, Skype uses encryption, making it difficult to decode bits of conversation. The encryption keys are not stored in the system but are immediately destroyed when the key encodes are transmitted. (refer to article on Skype, page 14.)

² (www.vonage.com, March 2004)



to broaden the class of information services, under the Telecommunications Act of 1996 in an effort to deregulate the industry and promote competition. For example, the Pulver.com Free World Dial-up service has been classified as an information service.

Currently, the FCC is engaged in several proceedings about the regulatory status of broadband Internet access services, IP-enabled services (including VoIP), and the applicability and implementation of CALEA. These proceedings may clarify the electronic surveillance capability assistance requirements that must be met by the various VoIP providers.

b2
b7E

—conclusion

Communications technology is rapidly providing anytime/anywhere services.



—current legal issues

The uncertainty regarding classification of providers as either “telecommunications carriers” subject to CALEA or exempt “information services” is compounded by the fact that these same terms, telecommunications carriers and information service, are used to define regulated and non regulated services under the Telecommunications Act of 1996. Moreover, the FCC has recently sought

As the telephone and information industries converge, the FCC, law enforcement, and service providers will need to work together to address law enforcement surveillance needs.

3. Service Provider Highlight—AT&T CallVantageSM

—executive summary

VoIP technology, enabling users to make and receive phone calls over high-speed data network connections, is becoming a popular alternative to traditional telephony services. Telecommunications companies are now offering VoIP services in addition to traditional phone services using analog twisted pair access. AT&T recently announced expansion of its enterprise VoIP services to residential customers, with plans to expand the service into 100 major markets by the end of the year. The company expects to sign up 1 million¹ business and retail customers by year-end 2005.

For residential customers, AT&T offers VoIP through a service called CallVantageSM.² Customers connect to this service through an adapter connected to their existing broadband Internet connection. The service gives customers the ability to make and receive phone calls with advanced features supported by a broadband connection, including call management.

For businesses, AT&T offers various services assisting businesses in the migration to a converged data and telephony network. AT&T’s Managed Internet Service (MIS) with VoIP service combines data, voice, and fax communications over the same network. AT&T also offers businesses a virtual private network (VPN) connection through its network-based IP VPN with VoIP offering.

—home VoIP—CallVantage

CallVantage gives users the capability to make and receive telephone calls with their existing telephone sets over their broadband Internet connection. In the home, the connection path is as follows:

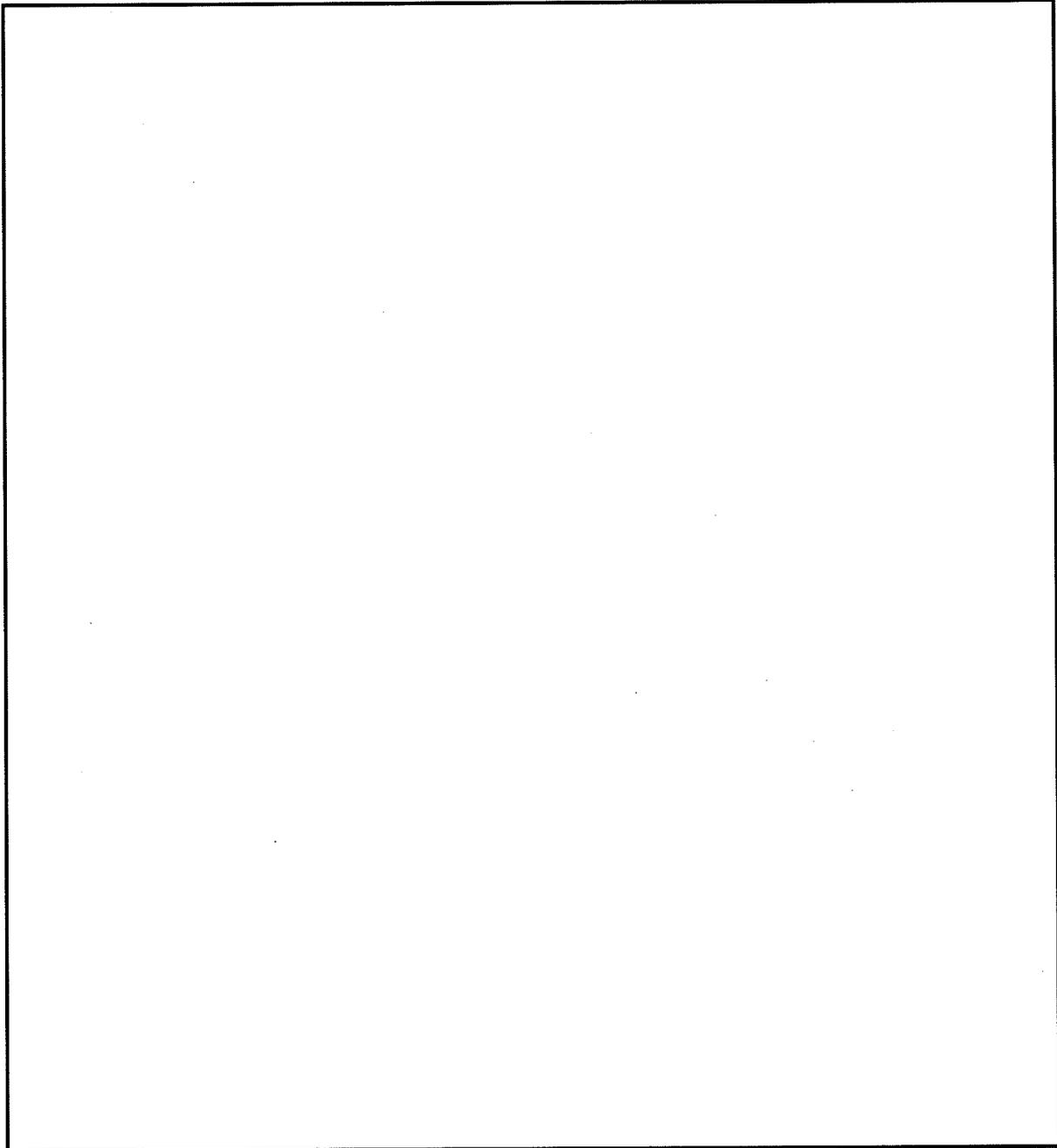


¹Vonage, a VoIP-only service provider, has in excess of 135,000 lines in service and is acquiring approximately 20,000 new lines per month.
²Additional information on the service is available at www.usa.att.com/callvantage/home.jsp

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL

b2
b7E

**How The Transition To IP-Based Communications Will Impact Law Enforcement's
Collection Of Audio Evidence – Talking Points**



**INVESTIGATIVE TECHNOLOGY DIVISION (ITD)
ELECTRONIC SURVEILLANCE STRATEGIC FRAMEWORK**

b2
b7E

I. Introduction

The information below summarizes the strategic approach identified by the Investigative Technology Division (ITD) for

II. Problem Description

III. Enforcement of Existing Law

Title 18 Action: "Show Cause"

Timeframe: Ad hoc

Title 50 Action:

Timeframe: Ad hoc

CALEA Action: NA

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL

IV. Legislation

V. Industry Liaison

Action: Industry Outreach

Timeframe: (Input required)

VI. Law Enforcement Cooperation

VII. Third Party

VIII. ELSUR Technology

IX. Standards

N/A

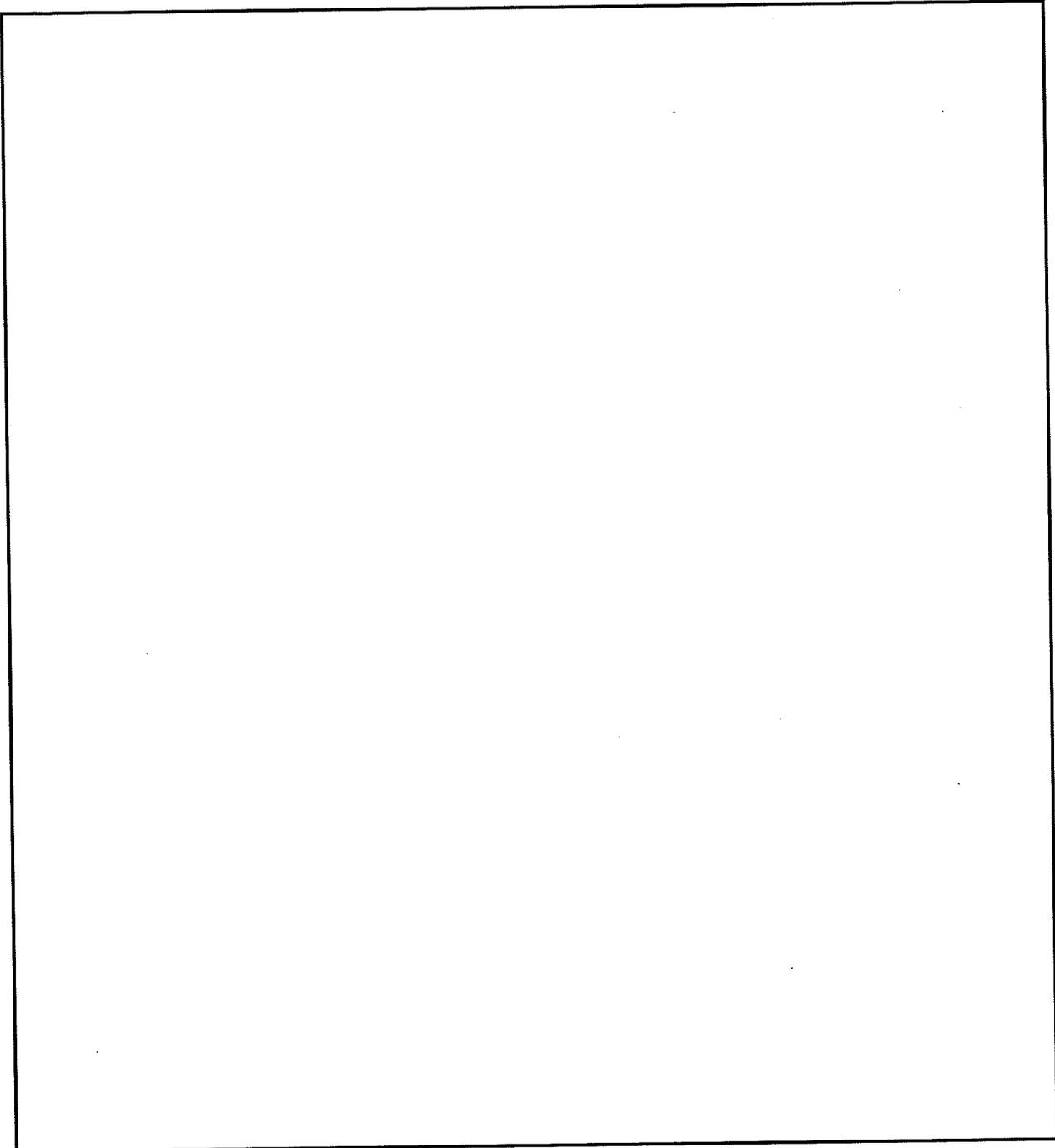
X. Additional Resources

Personnel Action:

Non-personnel Action:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-02-2008 BY 60322/UCLRP/PJ/EHL

**Communications Assistance for Law Enforcement Act (CALEA) Implementation Unit
(CIU)
Funding Request Description**



b2
b7E

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA)

FCC Notice of Proposed Rulemaking (NPRM) Addressing the Implementation of CALEA and Recent CNET News.com Article Entitled "Fahrenheit FBI"

I. BACKGROUND

Congress enacted CALEA in 1994 to help the nation's law enforcement community maintain its ability to use court-authorized electronic surveillance as an important investigative tool in an era of new telecommunications technologies and services.

On March 10, 2004, the Department of Justice, including the FBI, and DEA, on behalf of the law enforcement community, filed a Joint Petition before the FCC for expedited rulemaking to resolve various outstanding issues associated with the implementation of CALEA.

On August 9, 2004, the FCC released its CALEA Notice of Proposed Rulemaking addressing many of the issues raised in the Joint Petition. Also on August 9, an article written by Declan McCullagh entitled *Fahrenheit FBI* was published by c|net News.com (the entire article is available online at http://news.com.com/Fahrenheit+FBI/2010-7352_3-5300198.html). In the article, Mr. McCullagh asserts a number of common misrepresentations regarding the Joint Petition, the NPRM, and CALEA itself. The remainder of this document corrects and clarifies the statements in *Fahrenheit FBI*.

II. SETTING THE RECORD STRAIGHT

The very first sentence of the article, "*A new U.S. government decision extending wiretapping regulations to the Internet raises far more questions than it answers,*" perpetuates the myth that the Joint Petition requested the FCC determine the scope of CALEA extends to the Internet. In reality, the Joint Petition requested the FCC confirm that "broadband access" and "broadband telephony" are subject to CALEA. The Petition maintains the service made available by broadband access providers (i.e., transmission and/or switching of information, albeit at a high rate of speed) falls within the scope of services covered by CALEA. Broadband telephony refers to the transmission or switching of voice communications using broadband facilities. Both kinds of broadband are examples of services using packet-mode technology - technology in which communications are divided into packets before they are sent, transmitted individually, and recompiled into the original message once the packets arrive at their destination.

The article proceeds to portray the FCC NPRM as a decision to "*prohibit businesses from offering broadband or Internet phone service unless they provide police with backdoors for wiretapping access.*" On the contrary, the Petition did not, and the FBI could not, request any such power. Only the FCC has the authority to determine the services to which CALEA applies. What the Petition requested was greater accountability for the industry. Following a determination by the FCC that a service falls within the scope of CALEA, the FBI believes service providers should document their CALEA compliance to the FCC to ensure that new services do not offer havens for criminals and terrorists to communicate.

Fahrenheit FBI bluntly states the Petition requested the FCC “force surveillance back doors into instant-messaging programs.” The Petition neither requested, nor does the FBI believe, services such as instant messaging fall under the scope of CALEA. Other services frequently represented by the media as included within the Petition are pulver.com, Skype, Microsoft's Xbox Live gaming service, e-mail service, and visits to Web sites. Again, the Petition only requested the FCC confirm that “broadband access” and “broadband telephony” are subject to CALEA.

The article proceeds to ask a series of questions, some of which are CALEA-related, others of which are not. The remainder of this document identifies the questions and provides responses.

“Your request to the FCC said that broadband and VoIP companies may raise prices to ‘recover their CALEA implementation costs from their customers.’ How do you square higher prices with President Bush's speech in March calling for “affordable broadband” for all Americans?”

The industry has offered no evidence that addressing law enforcement's electronic surveillance needs will result in significant capital outlays for individual service providers. CALEA itself allows for service provider to recoup their CALEA compliance costs by passing them onto ratepayers. The Petition simply requests the FCC to formalize the rules by which service providers can choose that option. Further, there exist a small number of service providers that are compliant with CALEA, having received no CALEA-related reimbursement. The rates of these providers are no higher than those of their non-compliant competition.

“Congress gave telephone companies \$500 million to buy new equipment to comply with CALEA. Why should Internet companies not receive the same treatment? Is it because Verizon, SBC and the other former Bells have well-connected lobbying outposts in Washington, D.C.--but Vonage, 8x8 and other VoIP start-ups do not?”

The \$500 million was for equipment facilities and service already installed at the time CALEA was passed and before law was effective. Congress considered it only fair to provide subsidies for those upgrades. Having had nearly ten years to plan to meet law enforcement's electronic surveillance requirements, the same considerations don't apply to new and developing services, whether provided by traditional phone companies or others.

Skype CEO Niklas Zennstrom told me last fall that “we do not have any legal obligation to provide any means for interception” in his company's VoIP software. How will you force a company based in Luxembourg to insert backdoors in its software when it has no obligation to do so?

As stated above, the Petition did not request CALEA coverage of services such as Skype. The nature of the service, peer-to-peer technology, not its national origin, shapes the FBI's opinion of whether it falls within the scope of CALEA.

Even if Skype redesigned its software to satisfy the FBI, how would you stop its users from switching to a competitor that offered secure communications without back doors for police

surveillance? Why would criminals, terrorists and other miscreants choose to use eavesdropping-enabled software if a secure option was available?

The Petition did not request software applications such as Skype to be covered by CALEA. Law enforcement will need to employ other methods of conducting lawfully authorized electronic surveillance against threats to our nation utilizing application-based communications.

The FBI rarely gives up when it comes to demanding eavesdropping access. Your predecessors Louis Freeh and Janet Reno strong-armed Congress into approving CALEA on Oct. 7, 1994, one day before politicians left town for a fall recess. Capitol Hill is already considering VoIP regulation--will the FBI now ask Congress for regulatory power over peer-to-peer VoIP applications and instant messaging?

Congress is indeed already considering VoIP regulation – or more accurately it is considering legislation that would make VoIP free from much of the regulation that is imposed on traditional telephone services. The most recent example of such proposed legislation is the VoIP Regulatory Freedom Act of 2004. In its final form, as reported out by the Senate Commerce Committee, the Bill recognizes the need for law enforcement access to communications.

The popular SourceForge.net site lists dozens of free VoIP applications and programming libraries without FBI back doors. Fortunately for you, SourceForge.net is run by VA Software of Fremont, Calif., and is under U.S. jurisdiction. Should VA Software be permitted to continue distributing VoIP programs that don't guarantee access to the FBI?

This question is outside the scope of the NPRM and CALEA. The FBI has no authority to prohibit the distribution of any of the applications and programming libraries made available on any website.

Skype, PGPfone, and the still-incomplete GPGfone intentionally glue encryption into their VoIP applications to make them untappable. Your predecessor, Louis Freeh, lobbied Congress to ban strong encryption, and one House of Representatives committee agreed to his proposal in 1997. Will you pick up where he left off?

This question is also outside the scope of the NPRM and CALEA. Encryption poses certain challenges to law enforcement's efforts to conduct effective electronic surveillance. However, the FBI recognizes any Congressional decision regarding encryption will be made after its careful deliberation of a host of considerations of which law enforcement's needs are but one.

Conservative groups including Americans for Tax Reform, the Free Congress Foundation and the Rutherford Institute warn that granting your requests would "drive up costs, impair and delay innovation, threaten privacy and force development of the latest Internet innovations offshore." These groups share President Bush's commitment to the war on terror and backed you, John Ashcroft, when your nomination to be attorney general was foundering in the Senate. When they suggest other ways to accomplish your stated goal of protecting America, might they be right?

There is no evidence of the claim that CALEA would "*drive up costs, impair and delay innovation, threaten privacy and force development of the latest Internet innovations offshore.*" On the contrary, CALEA solution vendors have verbally advised that industry will find it much cheaper to bring its packet mode networks into compliance than it was to bring its circuit mode networks into compliance. The fact that several packet mode providers are currently complying with CALEA, suggests that CALEA compliance is not prohibitively expensive for them.

To the extent the cost of compliance may be onerous for other providers, CALEA provides them with "safety valve" protections. Rather than driving businesses off-shore, prohibitive costs, if indeed they exist, will result in those carriers being exempt from CALEA or will require that the government assume part of their financial burden.

Two of the FCC's five commissioners expressed reservations about the legality of extending CALEA to broadband and certain VoIP services. Commissioner Michael Copps warned: "If these proposals become the rules and reasons we have to defend in court, we may find ourselves making a stand on very shaky ground." Do you think that the FCC has the authority to extend CALEA to the Internet, given that Congress explicitly rejected that notion a decade ago?

The article misrepresents the statements of the Commissioners. The two FCC Commissioners to which the article refers believe that CALEA *should* apply to broadband and certain VoIP services, but they believe the argument is even stronger than the Commission's consensus NPRM. As stated above, the FCC was not requested to extend CALEA to the Internet. Rather, the Petition only requested the FCC confirm that "broadband access" and "broadband telephony" are subject to CALEA.

You've been saying that terrorists may use VoIP services to "evade lawful electronic surveillance." But the only detailed court statistics available show that 77 percent of wiretap applications were for drug crimes, and terrorism-related offenses were so few they didn't even make the chart. Is terrorism the real reason behind your wiretap push?

The statistics referred to in the article are based on the annual Wiretap Report, published by the Administrative Office of the United States Courts. It only accounts for wiretaps associated with criminal wiretaps, not those conducted under the authority of the Foreign Intelligence Surveillance Act (FISA).

The best figures available show that only 4 percent of wiretaps were targeted at computers and electronic devices last year, with the rest aimed at the traditional phone network. Vonage and other VoIP companies have pledged to work with you. Given that VoIP and instant-messaging clients aren't widely used yet, why not try the voluntary approach before talking about banning certain technologies?

Some carriers are good corporate citizens and others are not. A vital national security mandate such as CALEA cannot be left to corporate goodwill, especially in this age of increased threats to our homeland security. Congress recognized long ago that certain law enforcement assistance

must be ensured through a federal mandate. That is why CALEA was enacted and remains good law today.

American technology companies would like to help the FBI with legitimate investigations done under proper judicial oversight. But CALEA's requirements go hand in hand with the Patriot Act, which expanded the circumstances under which police may obtain wiretaps without a judge's prior approval. What assurances can you provide that the substantial powers you're seeking won't be abused?

CALEA contains built-in privacy protections that do not exist when law enforcement seeks to intercept a communication facilitated by a service or carrier that is not specifically covered by CALEA. For example, CALEA Section 105 requires carriers to follow certain surveillance provisioning procedures that protect the privacy of customers subject to lawful surveillance. Similarly, CALEA Section 103 requires carriers to "isolate" the communications of the targeted customer and only then to deliver those isolated communications to law enforcement.

CALEA itself does nothing to authorize interceptions of communications. The statute simply ensures that law enforcement has the technical capability to conduct the surveillance that has been authorized by a court, pursuant to other statutory authority. Surveillance authority and surveillance capability must go hand-in-hand.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-10-2008 BY 60322/UCLRP/PJ/EHL

Federal Bureau of Investigation
Fiscal Year (FY) 2009-2013
Internal Planning & Budget Review
Program Narrative Summary

(U) Division:	Operational Technology Division
(U) Section:	
(U) Program:	
(U) Strategy Map Objective(s):	A2, P3, ... Add others as needed

(U) I. FY 2009 BASE RESOURCES

(U) IA. Program Purpose. State the purpose and mission of the program.

Manage and operate National Program Office supporting LE communities to conduct LI on the Next Generation Networks efficiently and cost effectively.

(U) IB. Problem Assessment. Provide a description and assessment of the national security threat(s), crime problem(s), interest(s), and/or need(s) to be addressed by this program in the 2009 – 2013 timeframe. Please be succinct (no more than two pages) in this assessment/statement.

b2
b7E

(U) IE. Performance Measurement and Results. State what performance metrics are used to gauge the program's success. Provide evidence of the benefits derived from the program. Complete the following table to illustrate performance. Examples of workload/performance indicators could include cases addressed, arrests made, organizations dismantled, etc.

The performance metrics will be a major part of the NPO program. The NPO will support several internal audit functions for its offered services including QoS and QA.

WORKLOAD/PERFORMANCE TABLE								
Workload/ Performance Indicator	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007 Projected	FY 2008 Projected (assuming President's Budget)	FY 2009 Projected (assuming base resources)

(U) II. FIVE-YEAR PLANNING/END-STATE

IIA. Based upon your problem assessment, describe the capabilities this program will need to possess in order to accomplish its mission and deal with the problem(s) it is designed to address by 2013.

The NPO program must have the following capabilities to accomplish its mission:

<ul style="list-style-type: none"> a) b) c) d) e) 	Empty box for describing capabilities
--	---------------------------------------

b2
b7E

CLASSIFICATION (PLEASE CLASSIFY APPROPRIATELY)

- f)
- g)
- h)
- i)
- j)
- k)
- l)
- m)
- n)

(U) IIB. Identify the gap between these future capabilities and current capabilities.

- a)
- b)
- c) **Number of service providers and deployment of customized applications** etc.)
- d)
- e)
- f)
- g)

CLASSIFICATION (PLEASE CLASSIFY APPROPRIATELY)

5. Peer-to-Peer IP Services— Internet Telephony and Online Gaming

—executive summary

Peer-to-peer (P2P) communications are increasing in popularity. With P2P, users can establish a phone number through one of several central directory services (as done in traditional phone services), and exchange content directly through the network without the data passing through a central point.

Several P2P Internet telephony services are currently available as an alternative to the traditional circuit-switched phone system; some representative examples are SIPphone and Skype.

Another popular P2P application is online gaming. In late 2002, the online gaming industry had revenues of more than \$15 billion, making it more profitable than the U.S. movie industry. Studies indicate that online gaming will reach 114 million users worldwide by 2006. P2P online gaming technology can allow an unlimited number of players to communicate simultaneously over geographic borders without the use of a centralized host or server.

—technology/system

P2P technology allows users to connect directly with one another, enabling them to share files without going through a central host or server. Decentralized P2P systems are being adopted because they are more efficient than a client/server architecture and provide infinite scalability with decreased search time. Decentralized P2P systems also avoid the high cost and maintenance responsibility of centralized resources. Unlike centralized networks, where groups of users attach to network nodes, each user in a P2P network establishes itself as a node on the network and remains a node only when connected, virtually eliminating the costs associated with a large centralized infrastructure. When a user disconnects, there is no deregistration information provided to the network as there is in a PCS/cellular system.

¹SIP is a signaling protocol used for locating remote users and establishing interactive communications. It is analogous to setting up a call on the telephone network, with two critical improvements. It is Internet-native and therefore interoperates well with other protocols, including future protocols. It also separates session establishment and session description, so specifying the party with whom one would like to connect is independent of how one wishes to communicate. (Compare calling someone's voice versus fax line, where the choice of how to communicate dictates how one connects.) SIP is the glue for a new set of existing applications that go beyond IP telephony to include multimedia, mobility, instant messaging, e-commerce, Web services, and many others.

P2P technology is being widely adopted by companies wishing to establish data connections to a large number of users while minimizing central processing costs. Telephony is now viewed as a service that is easily adapted to a P2P architecture.

—SIPphone

SIP, or Session Initiation Protocol, is a protocol for establishing P2P communications between two network endpoints (e.g., computers, telephones) or to the PSTN through a VoIP gateway. SIP was envisioned as a means of establishing various forms of communications: voice, instant messaging, and exchanging data files. All can be shared using SIP without SIP servers managing the actual content of the communications. SIP is a far less complex call setup protocol than H.323 and is easy to deploy to establish almost any kind of communications between two network peers.

Among those providing SIP-based voice service is SIPphone Inc., a California-based company, which has announced the release of a VoIP product offering voice service using this protocol.¹ SIPphone's goal is to bring the benefit of SIP and free phone calls to a worldwide audience by offering plug-and-play hardware and an easy-to-use phone directory.



SIPphone sells an adapter unit allowing customers to use a standard analog phone for calls. The RJ45 connection on the adapter provides broadband connectivity to the user's ISP. The products are configured with a permanently assigned 747-area-code phone number regardless of where the user might be located. Purchasers, upon receipt of the equipment, connect to their broadband router and existing analog telephones and are immediately able to make calls to other phones using SIP. This equipment is relatively inexpensive. (Today the cost for two call-ready phones is approximately \$130.)

b2
b7E

Provisioning is maintained with SIPphone Inc., which includes the service directory and connections to the PSTN for limited² callout access. Other features include voice mail and conference calling. A user may set up such conference calls by selecting and calling a seven-digit number preceded by "1-222" (for example, 1-222-123-4567). If the number is available, then the user should hear a repeating welcome message. Associates will then call the same 1-222 number from their own SIPphones. Each person who calls the number will be automatically connected to the conference. SIPphone users are given a list of available 1-222 conference numbers to use for this conference service.³

SIPphone currently offers access to other SIP-based phone networks, including Free World Dialing (FWD) 393,

IPtel-477, and laxtel-700, and to PSTN toll-free numbers. In addition, subscribers wishing to connect to PSTN phones may connect using a prepaid card through toll-free access services.

—SKYPE

While SIPphone offers phone service provisioning through a central database, this is not the case for a service offered by the creators of KaZaA⁴ with its product Skype. Skype is based on P2P communications using a distributed user database for connectivity with up to five-user call conferencing. The software works with all firewalls, Network Address Translators (NAT), and routers and can function through dial-up as well as broadband connections.

—SIP call setup

Establishing a call illustrates the limited data needed to establish a communications session. Below is an example of a user placing a voice call in a manner similar to a PSTN call.

Establishing a Call

- » Both phones register with their respective SIP proxy servers. Note that this step does not happen once per call but rather at the initiation of service.
- » When connected to the service, both phones receive a "200 OK" message from the respective SIP proxies indicating that registration succeeded.
- » When a Subject Phone "A" wishes to connect to an Associate Phone "B", Subject Phone "A" sends an INVITE to Proxy "A". The INVITE includes SDP information specifying the media parameters this node supports / desires, including codecs, ports, and IP address for the streams.
- » Using DNS lookups, Proxy "A" determines that Proxy "B" is authoritative for the SIP URI being called, and forwards the INVITE to it.
- » Concurrently with the INVITE being forwarded to Proxy "B", a "100 TRYING" message is sent back to Subject Phone "A".
- » Proxy "B" receives the INVITE, checks to see if Associate Phone "B" is currently registered, and if so passes the INVITE to Associate Phone "B".
- » Associate Phone "B" accepts the INVITE, and returns a "180 RINGING" message back to Proxy "B".
- » Proxy "B" forwards the "180 RINGING" message back to Proxy "A".

- » Proxy "A" forwards the "180 RINGING" to Subject Phone "A".
- » The Associate finally picks up Phone "B", accepting the call and a 200 OK message is sent to Proxy "B". The "200 OK" message includes SDP information specifying the media parameters this node supports / desires, including codecs, ports, and the IP address for the streams.
- » Proxy "B" forwards the 200 OK message back to Proxy "A".
- » Proxy "A" forwards the 200 OK message back to Subject Phone "A".
- » Subject Phone "A" returns an ACK to Proxy "A". The ACK message may include SDP media information.
- » Proxy "A" forwards the ACK to Proxy "B".
- » Proxy "B" forwards the ACK to Associate Phone "B".
- » The two phones connect using the IP addresses passed during the session initiation.

The two phones are now communicating directly with each other using the public Internet or private managed network. The SIP proxies are no longer involved and the server ends the session and awaits the next request for session initiation.

[REDACTED] The direct communications between peers is the primary reason that a SIP infrastructure can be rolled out on minimal hardware: the SIP proxies are only involved in call setup. (Figure 5a provides a basic illustration of a SIP phone call setup for a phone using SIP.)

b2
b7E

²Toll-free numbers including calling cards.

⁴KaZaA is a P2P file sharing service.

b2
b7E

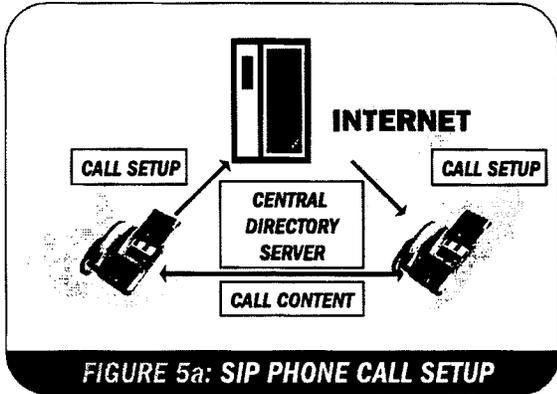


FIGURE 5a: SIP PHONE CALL SETUP

—online gaming

In discussions of online gaming, two types are typically considered. The first is a console that has the gaming software embedded within the device; the second is a console connected to a network in a client/server environment. In the latter case, a portion, if not all, of the gaming software resides on a server and devices interact with peers through a server. The client/server architecture allows peers in different locations to connect through the server to play the game. Online gaming has become so popular that networks are hard-pressed to handle the additional data traffic, resulting in game latency from the data bottlenecks. Because reaction time can win or lose a game, this reduction in network speed has motivated developers to consider alternative approaches to the client/server environment.

One response has been a move toward P2P networking. With P2P, the central server is no longer needed. The gaming console (peer) connects directly to another peer, relieving the data congestion produced in the client/server environment.

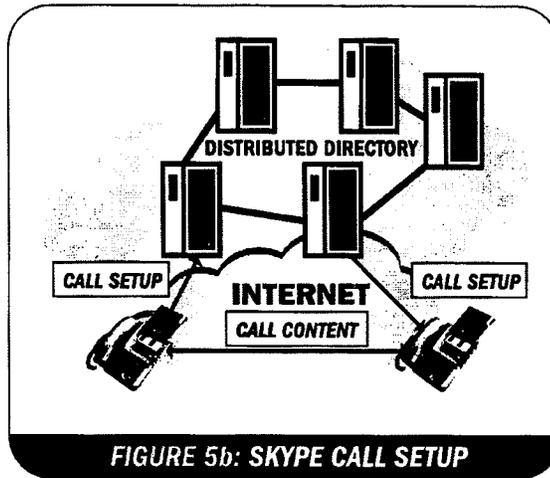
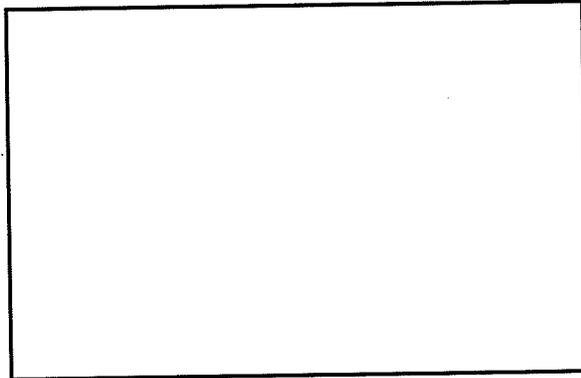


FIGURE 5b: SKYPE CALL SETUP

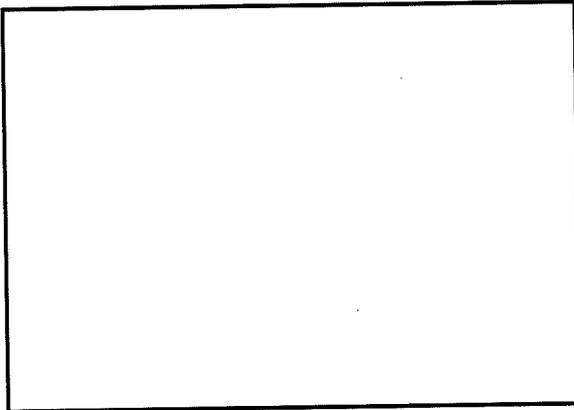
⁵According to the Skype Web site, the Skype program can be translated into any language. Skype encourages users to create and share translated language files (.lang) to help non-English speakers use the program. To translate Skype, a user chooses "Edit Skype Language File" from the Tools menu. A simple text editor will appear, showing the name of the items to be translated, the original version, and the translated text. Users then enter the new translated text for each item.



Consumers are buying into gaming on a large scale, with popular games attracting up to 450,000 subscribers at a time.⁷ With the global popularity of online gaming, there could be any number of players communicating with each other at a given time and any set of locations playing the game. In addition, with portable devices, there really is no restriction on where a game can be played. A player with a mobile phone in a park in Morocco, a player in a subway in Paris, and a player in an apartment in Madrid can all play a game against a player on a basement computer in the United States.

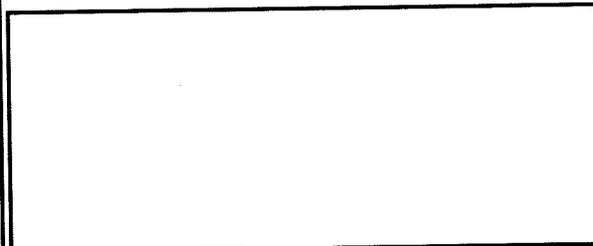


—issues for law enforcement



—conclusion

P2P technologies are becoming increasingly popular worldwide, and larger telecommunications companies are quickly realizing new potential.



b2
b7E

International telecommunications carriers also are becoming attracted to P2P technologies and are beginning to forge partnerships with some U.S.-based developers. The most recent example is Singapore Telecommunications Ltd.'s (SingTel) partnership with SIPphone to allow SIPphone user access to the PSTN and cell phone networks worldwide with use of a prepaid calling card.⁸

⁷(www.gamewatchers.net, June 2003)

⁸(www.singtel.com, April 2004)

[redacted] (OTD) (FBI) b6 b7C

From: [redacted] (OTD) (FBI) b2
Sent: Wednesday, November 15, 2006 3:34 PM b6
To: [redacted] (OTD) (FBI) b7C
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI) b7E
Subject: CALEA Test using [redacted]

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

Per our discussion, ETR has set up [redacted]

b2
b7E

It is our objective to [redacted]

b2
b7E

[redacted]

b2
b7E

ETR will report the findings if we observe issues for law enforcement.

[redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-10-2008 BY 60322/UCLRP/PJ/EHL

SENSITIVE BUT UNCLASSIFIED

[redacted] (OTD) (FBI) b6 b7C

From: [redacted] (OTD) (FBI)
Sent: Tuesday, January 16, 2007 9:54 AM b6 b7C
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: FW: Skype goes mobile

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-10-2008 BY 60322/UCLRP/PJ/EHL

FYI, b6 b7C
[redacted]

-----Original Message-----

From: [redacted] (OTD)(FBI)
Sent: Friday, January 12, 2007 3:01 PM b6 b7C
To: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI)
Subject: Skype goes mobile

UNCLASSIFIED
NON-RECORD

All, If you haven't seen this, I thought you might be interested. [redacted] b6 b7C

iSkoot, the service provider for mobile Internet (based in Cambridge, MA) announced this week that the iSkoot proprietary client software and its API has been Skype certified and it is available as free download software that can easily be integrated into most new mobile phones. This announcement confirms that iSkoot client software meets both mobile environment and Skype standards for usability and quality on the existing wireless networks. With iSkoot, VOIP users can take advantage of Internet phone services and buddy system to make unlimited VOIP calls using their P2P software from their cell phone.

This capability, when implemented in the mobile phones, allow users to make Skype calls (as well as other Skype services) on standard wireless networks. The iSkoot client software allows mobile users to place and receive Skype calls from their handsets, without the need for special hardware/software, PC or Wi-Fi/WiMAX or broadband Internet networks. The mobile user would benefit from all Skype supported features and services including P2P voice/data encryption and free phone calls when subscribed to Skype services.

According to iSkoot-Skype, the iSkoot client software currently supports Motorola Razor phones and Symbian-based mobile phones.

Current MS models supported are:

- Motorola (RAZR V3, SLVR L7, PEBL, v557)
- Nokia (6021, 6102, 6600, 6680, 6682, 6030)
- Sony Ericsson (v600i, w600i)

iSkoot also plans to support other Internet Protocol based services including Chat, IM, Google talk, Yahoo Messenger, and PC-based calling platforms.

It is estimated that there are more than 136 million Skype PC based user's worldwide using Skype PC client software for IP services. The iSkoot Skype wireless solution, when implementation could easily double the number of Skype wireless users in a very short time taking advantage of Skype features and "free" wireless services.

The iSkoot Skype API could be the next killer application in mobile environment!

Pulver.Communicator

Technology Update



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-10-2008 BY 60322/UCLRP/PJ/EHL

**OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research**

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

TECHNICAL ADDENDUM 4

TECHNOLOGY/ SERVICE 4

APPLICATION (USER SCENARIOS)..... 12

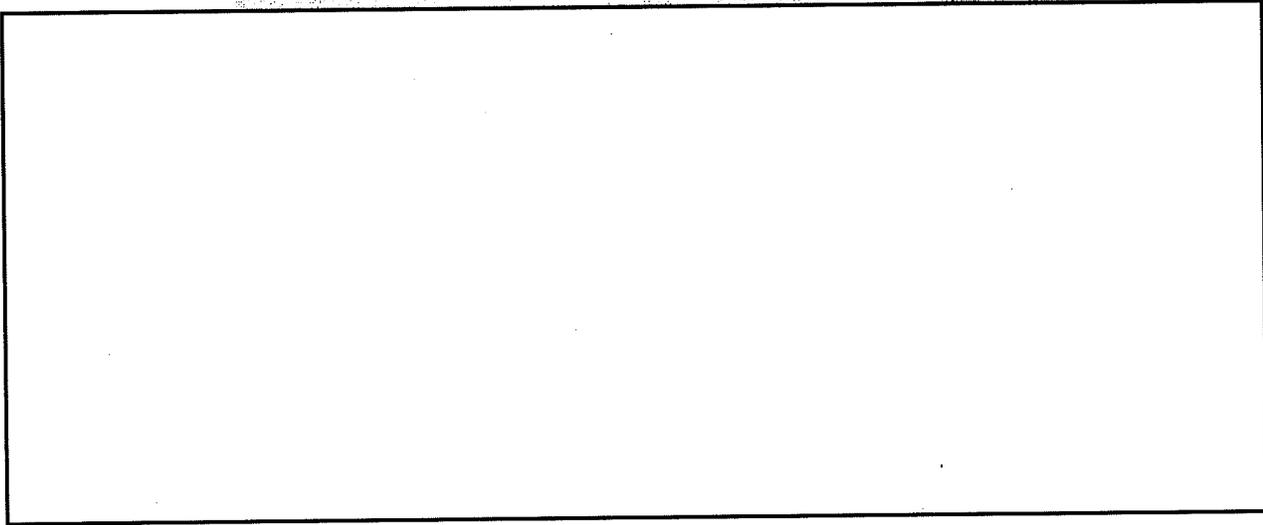
LAW ENFORCEMENT ISSUES..... 14

OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research

EXECUTIVE SUMMARY

The pulver.Communicator combines and leverages the advantages of all the best features of current leading edge IP applications in one Windows XP/2000 PC client application – Instant Messaging (IM), Voice over IP (VoIP), IP-voice conferencing, video calling, presence¹, and contact-sharing². It has the ability to integrate and communicate, one-on-one or multi-party, across the service boundaries of the four major IM networks (AOL, ICQ, MSN and Yahoo!). It enables users to share contact lists from all four services as well. VoIP connectivity is provided through the Free World Dialup (FWD) Communications Network and is extended by peering arrangements with over 80 VoIP providers worldwide including Skype, an extremely popular no-cost VoIP service with over 45 million users internationally. In addition, through a simple, no-cost download from pulver.com, pulver.Communicator was downloaded over 50,000 times within the first 3 months of its offering, and continues to expand its capabilities and business partnerships.

Pulver.Communicator uses Session Initiation Protocol (SIP) call setup to establish connect-via-hyperlink individual or mobile conference calls with SIP-enabled end points. Non-SIP enabled contacts can be sent a Call-Me Link enabling an immediate VoIP call-back to the sender via FWD Communication's FWDTalk service (see attached **Technical Addendum** for operational details). Anyone who has broadband internet access can today visit the FWD website, register with only a name, country, and e-mail address (names and locations are unconfirmed), and download the software at no charge. Within a few minutes they will have a FWD number assigned to them and be able to make and receive calls from all over the world. Two-way webcam video calling is a standard feature as well. The pulver.Communicator offers anyone with broadband access and a headset the ability to communicate internationally within a highly encrypted, decentralized, unregulated, worldwide network through service providers ranging from conglomerates like AOL and MSN to third-tier local VoIP providers only found overseas.



b2
b7E

¹ Presence – the ability to determine if contacts are present and able to be called.

² Contact-sharing – the ability to import and export contact lists from IP communication applications

OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research

TECHNOLOGY/SERVICE

Background

In October 2004, pulver.Communicator was launched by Free World Dial-up (FWD) Communications as a new application that combines IP communications such as IM, voice, video, presence, and social networking into one software platform, for expanded IP communications and conferencing among members using the supported applications listed below. It has been marketed to OEM makers of IP-enabled devices including PCs, PDAs, and cell phones for integration into their product designs, and is readily obtained by anybody with an online PC through a no-cost download and registration with the pulver.com website, so is widely available for use. The developer, Jeff Pulver, is continually seeking to establish additional business partnerships to expand the capabilities of the service and integrate it into mainstream computer usage worldwide.

Use of the pulver.Communicator requires a user ID, created from the setup of an account with FWD. The SIP-based network established connections with an array of both software and hardware IP phones (see below – **Free World Dialup Explained**³). The pulver.Communicator is considered a

³ **Free World Dialup (FWD) Explained:** Since its launch in November 2002, FWD has evolved as a communications network that offers compelling features and a large (several hundred thousand) subscriber community. It is not a closed PC-to-PC communications network. Anyone who has broadband internet access can today visit the FWD website, register with only a name, country, and e-mail address (names and locations are unconfirmed), and download the software. Within a few minutes they will have a FWD number assigned to them and be able to make and receive calls from all over the world. FWD is compatible with many commercial hardware-based IP telephones available in the marketplace, such as Grandstream, which is also available for sale on the FWD website.

Once a user is set up with his or her FWD number, they can combine with a number of other service providers to receive, for free, a US or International Direct-Inward-Dial (DID) number which is mapped to their FWD number. The impact of this service is that the new customer can then receive direct-dial phone calls from traditional home phones and cellular phones. In addition, there are free "gateway" services available in many countries which offer the ability for two-stage dialing from a regular telephone to a subscriber's broadband FWD phone number.

Within the FWD network, it is possible to place toll-free calls into the US and free phone calls into the many other supported countries. These services are made available through peering agreements with others that connect to the FWD network. If a subscriber has a friend with a toll-free number at their home or office, that friend can be reached from FWD. Also, FWD provides the services of an Instant Messaging network if configured with Windows Messenger 5.0. Basically, as long as someone has broadband internet access and can get to the FWD website, they can receive calls from "regular" phone networks within a few minutes. FWD offers the following advanced features for free: Voice Mail, Caller ID, Call Waiting, and Multiple Presence, among others. A subscriber may have more than one registered FWD accounts with phone numbers, but not one single account associated with more than one number. Also, FWD allows registration from many locations at the same time for the same account. When a call comes in, the system rings all the registered locations – the first one to answer is connected.

The current third generation of FWD is a 100% SIP based, peer-to-peer, end-to-end broadband IP solution designed for people who wish to use dedicated IP Phone devices or softphone SIP clients. FWD does not provide direct connectivity to the PSTN but rather connects people through third party service providers (such as LibreTel, which is heavily advertised on the FWD website) who can facilitate full connectivity to legacy telephone networks. Subscribers represent over 150 countries and the sound quality is better than cellular. The number of features and services that users can access continues to grow.

Source: Free World Dialup web site, http://www.freeworlddialup.com/corporate/about_fwd_1

**OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research**

software phone for use over the FWD network. FWD service went live on November 11, 2002, and delivers no cost calling to hundreds of thousands of members in over 180 countries. FWD access requires a broadband connection such as DSL or cable (any connection offering a bit rate higher than 100kps). Using the pulver.Communicator would only require the use of a computer meeting the system requirements, working off of Windows 2000 or XP platforms (under the latest Windows-compatible release, Beta Version 0.95.3). There is no requirement for a static IP address, and the software is configured to work around Network Address Translators (NATs) and firewalls. Currently, pulver.Communicator offers integration of the following PC communications applications:

Instant Messaging	VoIP	Other Capabilities
<ul style="list-style-type: none">• AOL Instant Messaging service (AIM)• Yahoo! Messenger• MSN Messenger• ICQ	<ul style="list-style-type: none">• Free World Dialup service• Over 80 Worldwide service providers, including Skype (Voice and IM)	<ul style="list-style-type: none">• Session Initiation Protocol (SIP) based networking• Really Simple Syndication (RSS) Feed downloads

Modes of Operation

While usage of pulver.Communicator for IM chat is fairly straightforward, as the application simply connects to each hosting company as does each company's traditional IM application (such as MSN Messenger or Yahoo! Messenger), however it also offers conference IM capability which may include not only AOL, MSN, ICQ, and Yahoo! IM users but also Skype contacts as well. The pulver.Communicator is able to make phone calls over IP as long as the computer it is being used on has the Windows XP/2000 operating system and a microphone and speakers, or a headset plugged into the appropriate jacks. IM sessions may be graduated to a phone call as long as all involved contacts have a telephone presence that is compatible with the application. One reason behind the development of pulver.Communicator is the previous reliance on softphone and hardphone vendors for FWD usage. With the release of pulver.Communicator, a single click can establish a person-to-person call with any online contact whether the contact is a FWD subscriber or not, as long as they have the proper software and hardware installed. Figures 1 through 10 show some screenshots of pulver.Communicator and examples of common type of usage.

OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research

Pulver.Communicator Call Scenario:

- Two users chatting over an IM session on pulver.Communicator:

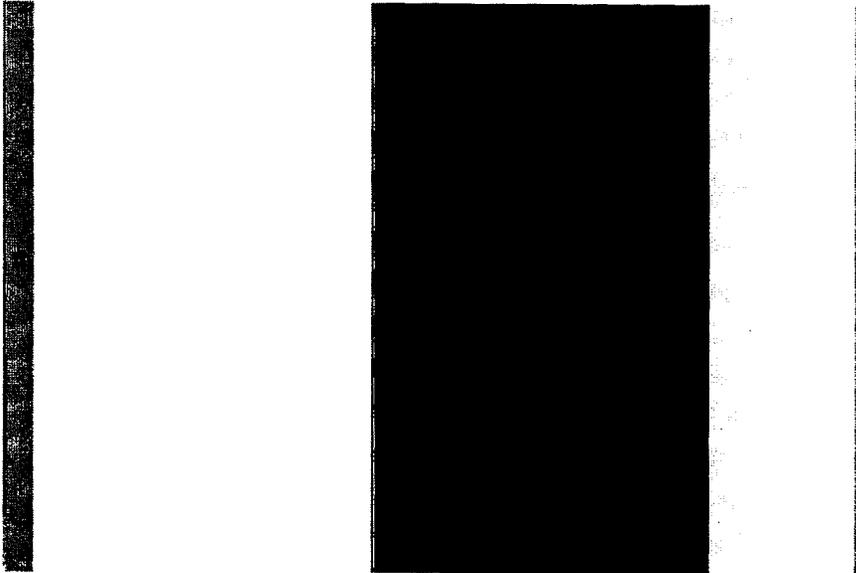


Fig. 1 - Instant Messaging session screenshot

- User A wishes to initiate a person-to-person call with User B. The call is established by clicking the “Call” button located in the upper left of the IM window. *This button is only present when the selected chat Buddy has a telephone presence that is recognized by pulver.Communicator:*

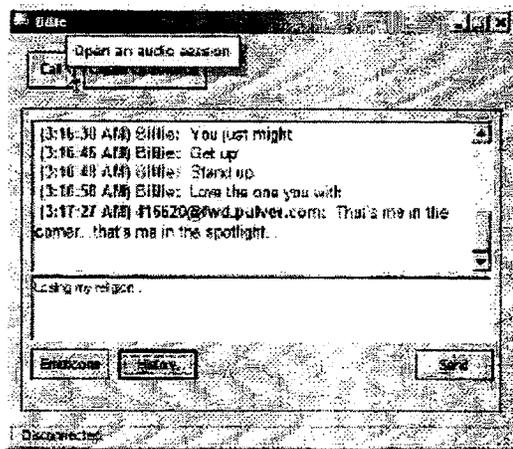


Fig. 2 - IM window with Call button being selected

**OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
 ADVANCED TELEPHONY UNIT
 Emerging Technologies Research**

- The IM dialog box extends to show phone controls (and a Buddy Image if configured by the contact) for speaker volume, microphone volume, display of a numeric dialpad, an End Call button and a Hold button:

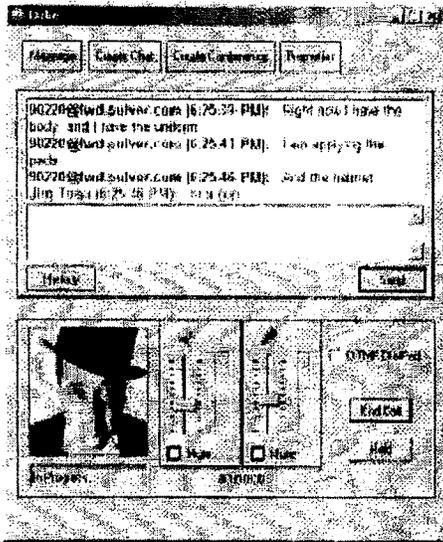


Fig. 3 - IM dialog box with call controls

- Each user could graduate the call to either a chat or conference call with other users by clicking the Create Chat or Create Conference buttons at the top of the IM window. Both calls and IM sessions may utilize conferencing with an undetermined number of users:

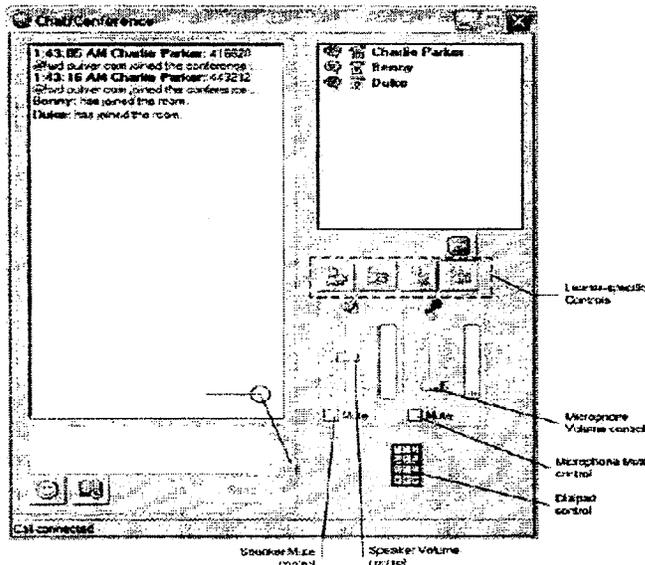


Fig. 4 - IM conference chat window with three users

**OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
 ADVANCED TELEPHONY UNIT
 Emerging Technologies Research**

- It is also possible to make a call directly without beginning from an IM session. By clicking on the Direct Dialing field at the bottom of the main pulver.Communicator window, the field will clear and a cursor will appear in the field, prepared for input of a FWD phone number (format ##### [i.e. 123456], plus country or partner service provider prefixes) for any of the SIP service providers with which FWD has a partnering agreement. Or, a SIP contact can simply be clicked upon and the call window will display:

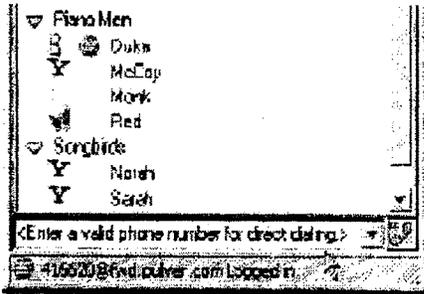


Fig. 5 - Direct Dialing Field at bottom of contact list

- Once entered, the Initiate Call icon to the right of the Direct Dialing field can be clicked, or the call can be initiated simply by pressing the Return key. A call window will display:

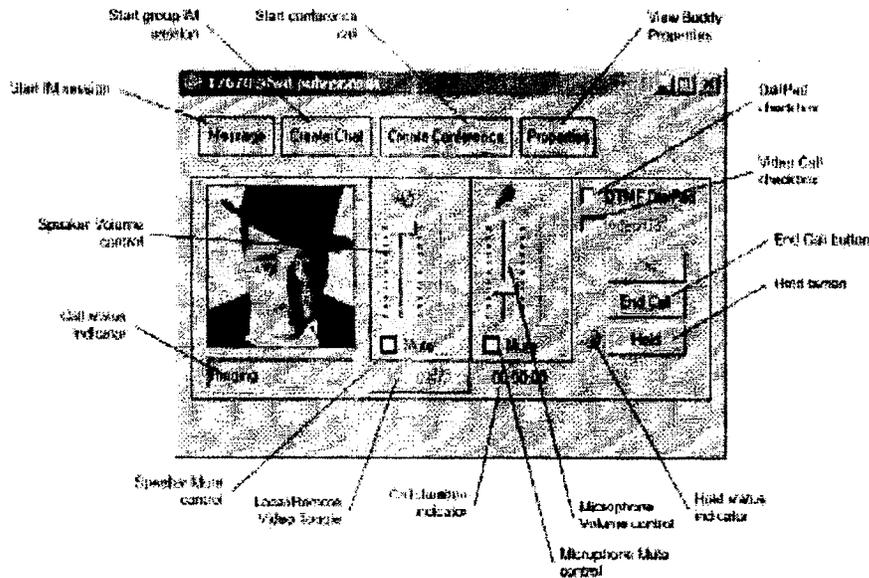


Fig. 6 - Call window with controls for Instant Messaging, Group IM Chat, Conferencing, Speaker Volume, Microphone Volume, Video Calls, End Call, and Hold

OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research

- Users can make calls with webcam video to Buddylist contacts by using the right-click menu on a contact's name, as shown.

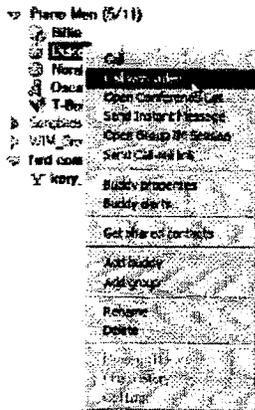
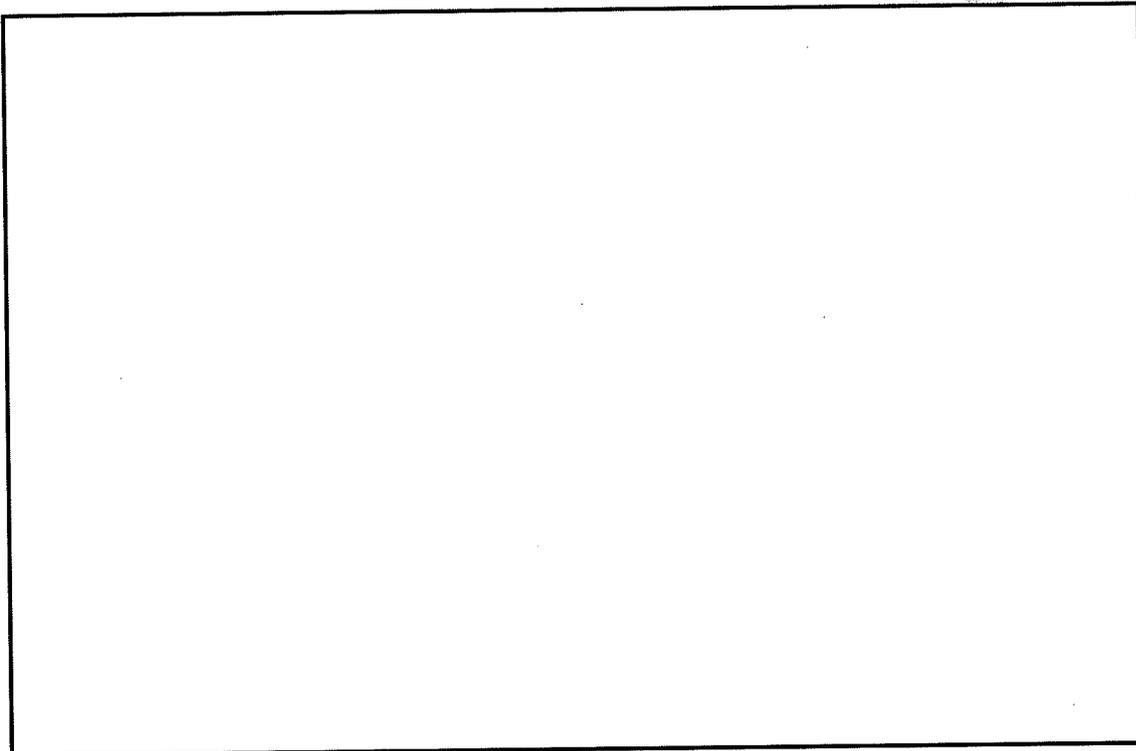


Fig. 7 - Initiation of a call with video

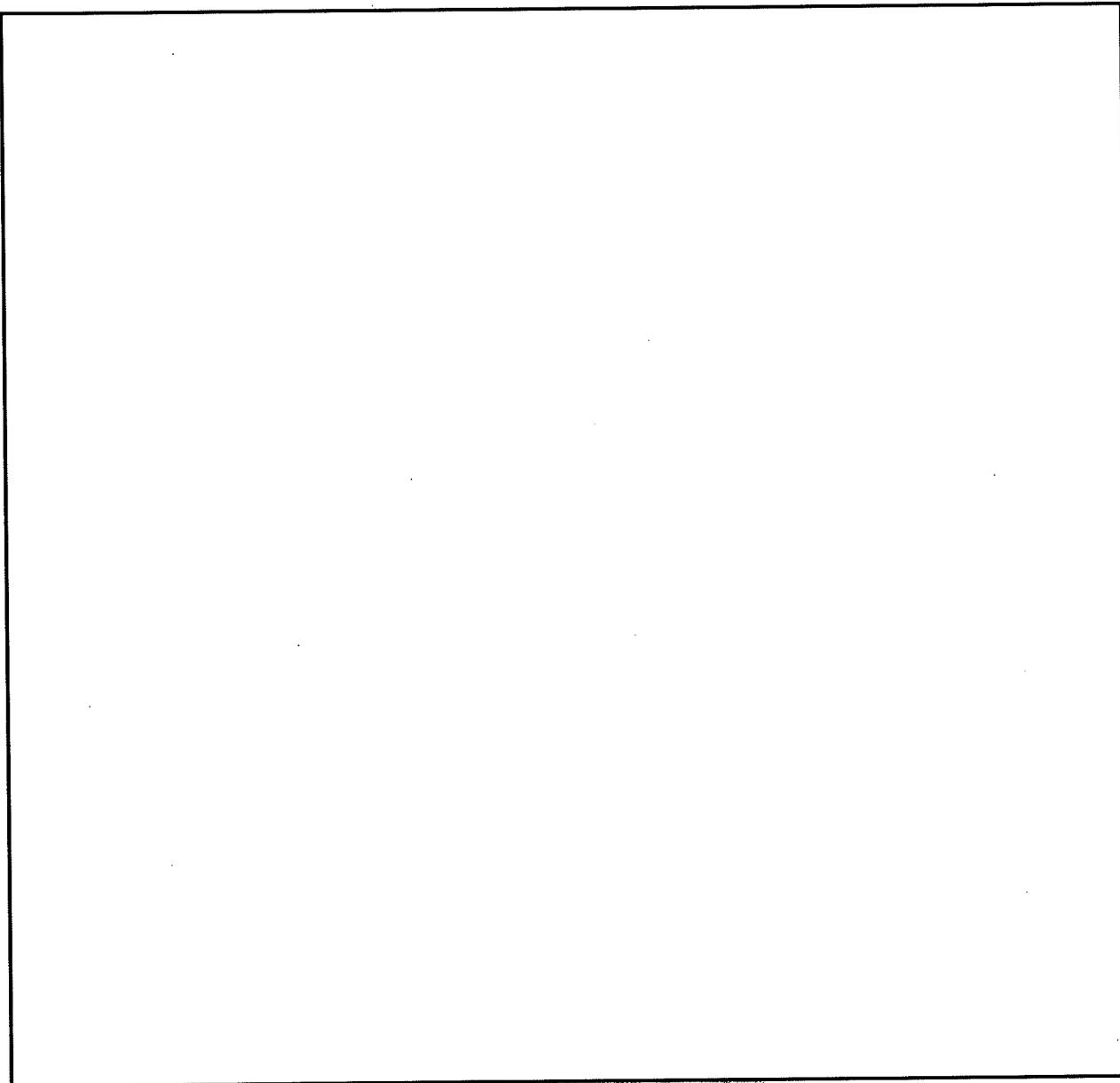
- The user selects "Call with video" from the dropdown menu and the call will commence with the same call window displayed as before, except in place of the Buddy Image there is live video from the broadcasting webcam instead.



hs
ne

b2
b7E

OID - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research



b2
b7E

Fig. 10 - Chat History dialog box

The pulver.Communicator will automatically import contacts from supported IM applications if they are installed on the user's PC, and will also do the same for Skype. SIP communication is possible through the mandatory FWD account, or users can purchase an unlocked version of the software to connect through any SIP-compliant network, such as AT&T, Bell Canada, GlobalNet, KyTEL, and MCI, among countless others. Also, users can now broadcast video to their SIP-

⁴ Complete setup and operational procedures for pulver.Communicator may be found online in the pulver.Communicator User's Guide at <http://communicator.pulver.com/documentation>.

OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research

enabled contacts via webcam and receive webcam video from those contacts as well. No specific webcam configuration is required.

Pulver.Communicator currently supports firewall traversal technologies uPnP, Direct Connections, and both STUN⁵ and NAT⁶ Connectivity. The application will not be limited to these technologies in the future, as new firewall techniques will continuously be integrated and improved to ensure user support and acceptance.

Related Facts

Collaboration with Skype, a VoIP service that is available for online download at no cost, tremendously impacts the potential usage of pulver.Communicator, since July 2005 Skype boasts over 45 million users internationally and 120,000 downloads per day for its free service. Additionally, Skype now offers connection to landline telephones via SkypeOut, where users can pay as low as two cents per minute for the ability to connect to traditional telephones in supported countries with prepaid credits through their account. [REDACTED]

[REDACTED] Another notable issue when dealing with Skype communications is its advanced encryption system. [REDACTED]

b2
b7E

There is a Skype login server which is where user names and passwords are stored and user authentication is performed. It also ensures Skype login names are unique across the Skype name space. However, apart from the login server, there is no central server in the Skype network. Since Skype is an overlay P2P network, any node (user) with a public IP address having sufficient CPU, memory, and network bandwidth is a candidate to become a super node, which is an ordinary host's endpoint on the Skype network and provides the ability to connect other P2P sessions. Online and offline user information is stored and propagated in a decentralized process, as are user search queries. It is believed that there is no global NAT or firewall traversal server being used by Skype, and that each node uses a variant of STUN protocol to determine the type of NAT and firewall it is behind.

⁵ STUN stands for "Simple Traversal of UDP over NATs", and is a network protocol which helps many types of software and hardware receive User Datagram Protocol (UDP) information properly through home broadband routers using Network Address Translation (NAT). In other words, it is a lightweight protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public internet, to determine the public IP address allocated to them by the NAT, and allows the applications to work through the existing NAT infrastructure.

⁶ NAT stands for "Network Address Translation", and is a technique in which the source and/or destination addresses of IP packets are rewritten as they pass through a router or firewall.

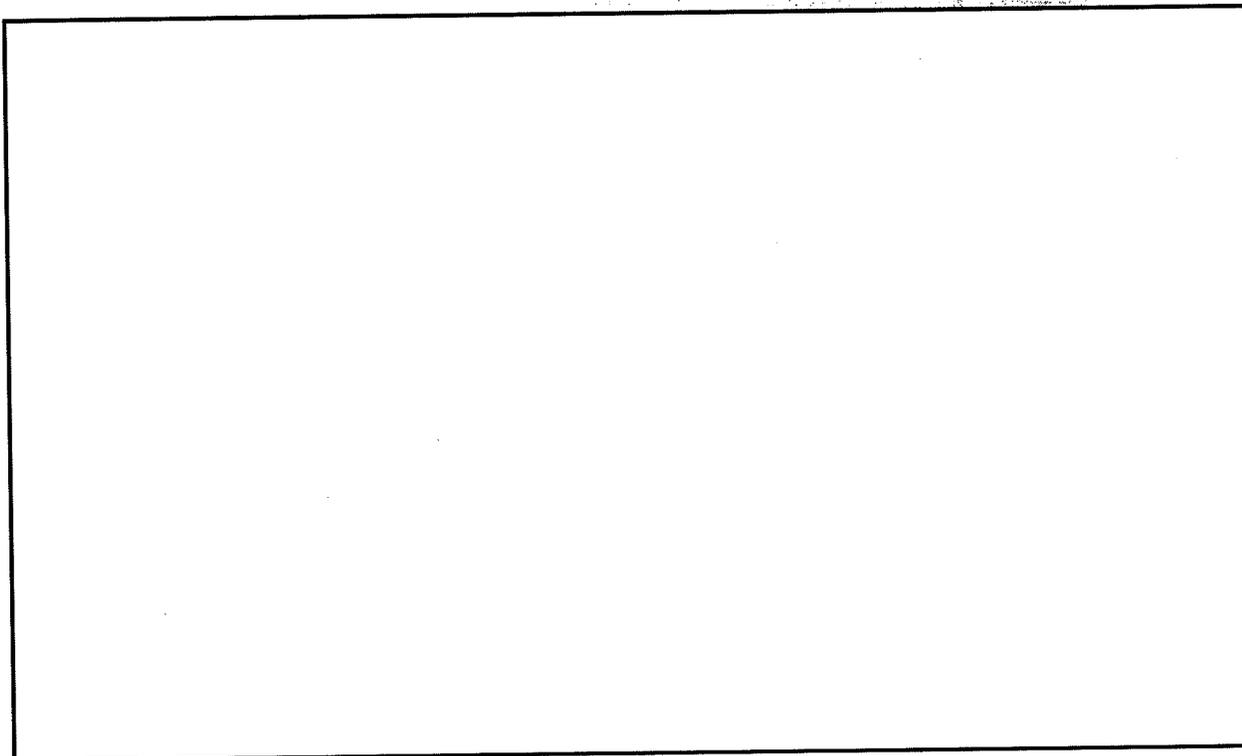
**OTD - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
 ADVANCED TELEPHONY UNIT
 Emerging Technologies Research**

Skype vs. All The Rest

		Net2Phone	MSN Messenger, ICQ, AIM, Yahoo Messenger	Other standard VoIP clients
Works with ANY firewall/NAT setup - nothing to configure				
Unlimited FREE calls to users of same application				Sometimes
Sound quality	 Better than phones	 Worse than phones	 Worse than phones	 Worse than phones
Secure and encrypted communications				
100% ad-free				Sometimes

Figure 11: Features of Skype vs. Other IP Communications Providers

APPLICATION (USER SCENARIOS)



b2
b7E

OID - ELECTRONIC SURVEILLANCE TECHNOLOGY SECTION
ADVANCED TELEPHONY UNIT
Emerging Technologies Research

b2
b7E

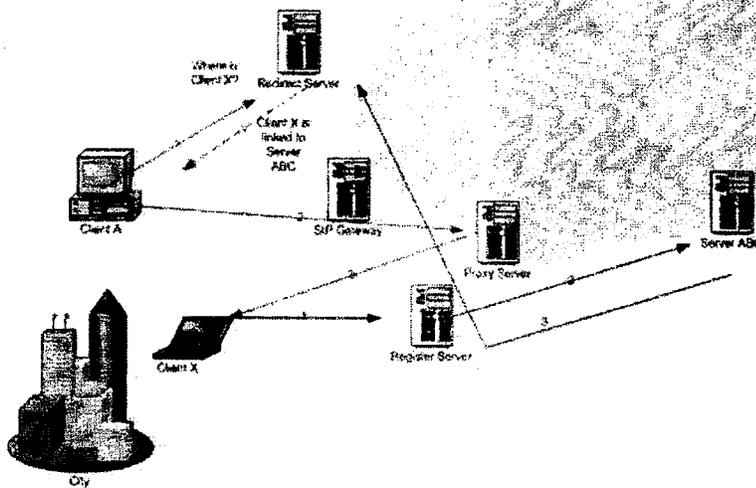


Figure 12: SIP Network Diagram

In the above diagram, the call flow is routed as follows:

1. Client X's login is verified at the Register Server
 2. The Register Server passes Client X's identification credentials to Server ABC
 3. The credentials are forwarded back through the Register Server and on to the Redirect Server to prepare for communication with Client A
-
1. Client A connects to the Redirect Server for locating information to establish a connection with Client X
 2. Client A sends a signal through the SIP Gateway and on to a Proxy Server which links with Client X
 3. The connection reaches Client X from the Proxy Server, establishing a direct link between Clients A and X for communication

ADVANCED TELEPHONY UNIT
Emerging Technologies Research

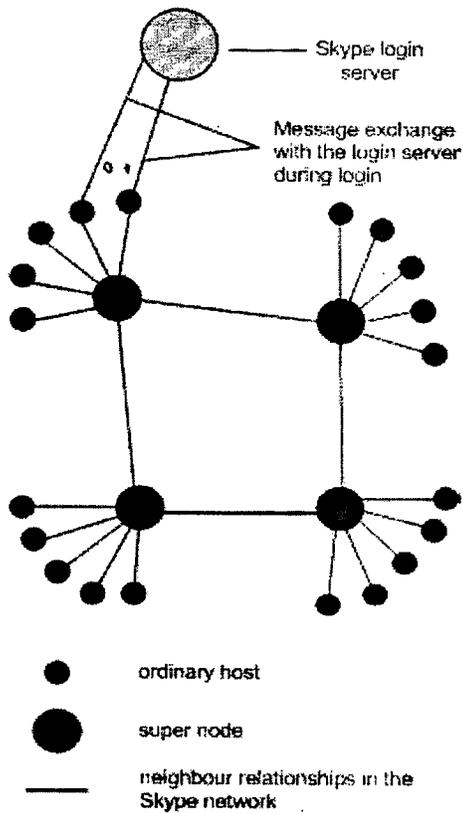
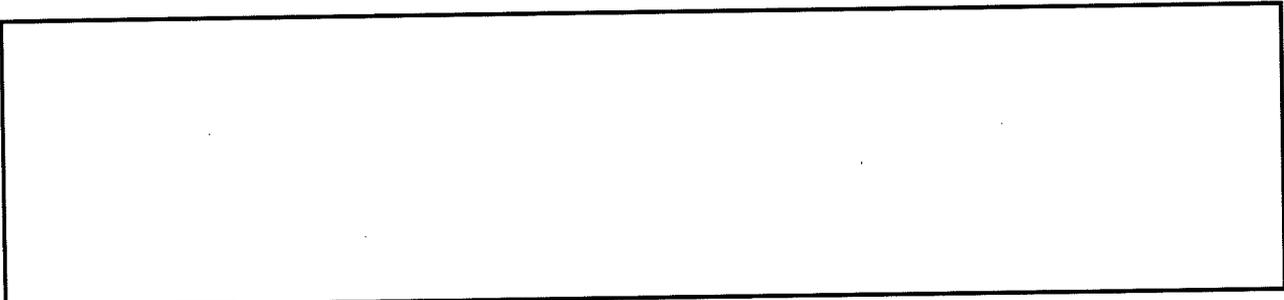


Figure 13: Skype Network Diagram

In the above diagram, the Skype network is illustrated showing the central Skype login server, where user IDs and passwords are authenticated via message exchange during login, as well as the hierarchy of nodes and super nodes. If a user is online and has the resources (CPU, memory, and network bandwidth) to operate as a super node, his machine may automatically be utilized as such. The user has no option to disable this function. An ordinary host must connect with a super node and register itself with the Skype login server for successful login. Apart from the login server, there is no central server within the Skype network.

LAW ENFORCEMENT ISSUES



b2
b7E

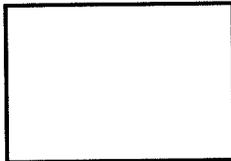
MEMORANDUM

VIA E-MAIL

TO: FBI/CALEA Implementation Unit
FBI/Office of General Counsel

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-11-2008 BY 60322/UCLRP/PJ/EHL

FROM:



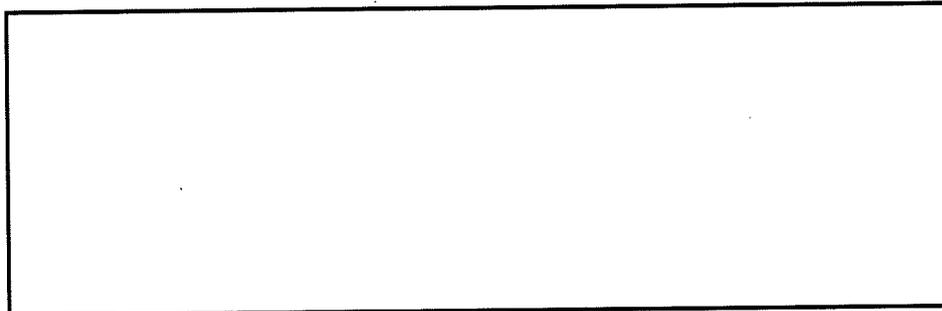
b6
b7C

DATE: June 29, 2004

RE: Proposed Outline for Reply Comments in the
IP-Enabled Services Proceeding

This memorandum contains our proposed outline for the DOJ's reply comments in the FCC's IP-Enabled Services notice of proposed rulemaking (hereinafter the "IP NPRM").¹ Please review the outline and provide any feedback to us **by close of business Wednesday, June 30th**. With your approval we will then circulate the outline to the DOJ Working Group. To save time we will start drafting the reply comments now. The FCC filing deadline is **Wednesday, July 14th**.

I. Regardless of Which Regulatory Classification the FCC Applies to IP-Enabled Services, Broadband Telephony Services Should be Subject to CALEA



b2
b5
b7E

¹ *In re IP-Enabled Services, Notice of Proposed Rulemaking*, WC Docket No. 04-36 (rel. March 10, 2004) (hereinafter "IP NPRM").

Privileged and Confidential
Protected by Attorney Client Privilege

VIA E-MAIL

To: [Redacted]

From: [Redacted]

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-11-2008 BY 60322/UCLRP/PJ/EHL

Date: April 2, 2004

Re: Proposed CALEA Legislation -- Scope of Coverage and Capability
Requirements

We have been asked by the FBI to prepare a memorandum [Redacted]

[Redacted]

I. Scope of Coverage

The goal of this section would be to ensure that [Redacted]

[Redacted]

b2
b5
b7E

Deleted: "

Deleted: -like"

Deleted: and "Excluded Services"

REMARKS FOR VON 2004

Good afternoon. My name is [REDACTED] and I'm a Special Supervisory Agent with the FBI's CALEA Implementation Unit. I'd like to devote my remarks today to the petition recently filed by Law Enforcement with the FCC seeking an update of the CALEA implementation rules. Based on certain media reports, the petition for CALEA rulemaking has fallen prey to seven different myths. But these myths can be readily dispelled. In fact, I think an accurate reading of the petition will reveal a set of proposals that are squarely within the law, appropriate for the needs of Law Enforcement, and not nearly as burdensome on industry as some would have you believe.

Myth number one: the CALEA petition seeks to apply CALEA to all types of IP-based communication services, including pulver.com, Skype, Microsoft's Xbox Live gaming service, e-mail service, instant messaging, and visits to Web sites. Actually, the CALEA petition did not propose CALEA coverage of any of those things. It proposed coverage of broadband Internet access service providers and certain broadband telephony service providers such as Vonage Holdings, Inc. Law Enforcement takes a different view toward pulver.com, Skype, and other pure peer-to-peer voice software developers because they rely on different architectures and perform different functions. Under the petition, e-mail and instant messaging would remain exempt from CALEA as "electronic messaging services," and the hosting of stored data files such as Web sites would remain an exempt "information service" under CALEA Section 102.

Myth number two: the CALEA petition exceeds the bounds of the statute because it would give Law Enforcement a right of prior approval over new communication services that interact with the Internet, thus stifling innovation in the nascent broadband industry. This is also untrue. The CALEA petition would permit the introduction of any new service or feature without prior approval by Law Enforcement. Moreover, carriers would continue to enjoy the right to adopt CALEA technical standards, either through public standard-setting bodies or through private arrangements with their respective equipment vendors.

The new concept introduced by the petition is one of accountability. Law Enforcement believes carriers should document their CALEA compliance at certain compliance benchmarks, just as the FCC already requires in the E911 program. Otherwise, the CALEA compliance process will continue to suffer from an endless cycle of routine, industry-wide extensions of time. Law Enforcement would have a right of "consultation" in the process, as set forth at CALEA Section 107, but decisions about whether a given carrier has missed a benchmark or met a benchmark in a non-compliant manner would be decided by the FCC, not by Law Enforcement.

Myth number three: Broadband carriers are information service providers and therefore exempt from CALEA. That legal issue remains very unsettled. If anything is certain, it is the FCC's express ruling that CALEA applies regardless of changes in technology. Under CALEA, it doesn't matter whether an entity provisions a phone call in narrowband or broadband mode. The CALEA obligations remain the same. Indeed, the whole purpose of CALEA is to help Law Enforcement keep pace with evolving telecommunications technologies when conducting lawful electronic surveillance. The current migration to broadband communications is just the kind of technological change where CALEA is supposed to apply.

Remember that the scope of CALEA coverage depends on the definitions of CALEA, not the definitions of the Communications Act. The FCC has expressly recognized this point. Even if the Commission finds this "dual-definition" theory insufficient to ensure CALEA coverage of

broadband providers, it has plenty of authority to ensure the needed coverage on other legal grounds.

Myth number four: Law Enforcement doesn't really need CALEA because it has already developed packet-mode intercept technologies of its own. Don't believe everything you see on T.V. shows like "The Threat Matrix," where agents and officers miraculously monitor suspects with the push of a button. Given the rapid evolution of telecommunications technology, the surveillance task will only become more difficult over time. If this nation is to have an up-to-date, efficient, reliable, cost-effective system of lawful electronic surveillance, industry must develop the solution. What's needed is for each telecommunications provider to take responsibility for its own facilities. That was the division of labor adopted by Congress in 1994, and that scheme is all the more necessary today.

Myth number five: Broadband service providers need not be subject to CALEA because they can be trusted to assist Law Enforcement through "voluntary efforts." In reality, some carriers are good corporate citizens and others are not. A vital national security mandate such as CALEA cannot be left to the whims of goodwill, especially in the age of Homeland Security. Congress recognized long ago that certain Law Enforcement assistance must be ensured through a federal mandate. That's why CALEA was enacted and remains good law today. Yes, some carriers claim they already assist Law Enforcement, but in some cases that means they do nothing more than provide customer records in response to Law Enforcement subpoenas. That is not electronic surveillance.

Of course, Law Enforcement continues to believe in cooperation with industry. Significant progress was made in the circuit-mode generation of CALEA though cooperative agreements and flexible deployment schedules negotiated between the FBI and a wide range of companies. Law Enforcement remains open to new mechanisms of cooperation today. Specifically, if a carrier approaches the FBI CALEA Implementation Unit with a good faith willingness to comply with the law, it may be surprised by the Unit's willingness to accommodate legitimate business needs. Despite the stereotype of the hard-nosed cop, the FBI has historically relied far more on industry relationship-building than it has on enforcement actions under CALEA Section 108.

Myth number six: the petition would impose excessive costs on industry. Law Enforcement has seen no evidence of this claim. On the contrary, CALEA solution vendors have verbally advised that industry will find it much cheaper to bring its packet-mode networks into compliance than it was to bring its circuit-mode networks into compliance. Also consider those packet-mode providers that say they are complying with CALEA voluntarily. If so, then CALEA compliance is not prohibitively expensive for them. And if the cost is not excessive for them, why would it be excessive for others? Of course, Law Enforcement recognizes that some small or rural carriers lack the financial resources of the big players. For them, CALEA already provides considerable flexibility. As long as the affected party can show the Commission that a certain CALEA capability is not reasonably achievable, whether for economic reasons or other reasons, the Commission already has the authority to remove the unwanted burden pursuant to CALEA Section 109.

Myth number seven: applying CALEA to packet-mode communications would infringe on customer privacy rights. Actually, a packet-mode provider that is covered by CALEA is subject to more privacy requirements than a non-covered provider because CALEA contains built-in privacy protections. For example, CALEA Section 105 requires carriers to follow certain surveillance provisioning procedures that protect the privacy of customers subject to lawful

surveillance. Similarly, CALEA Section 103 requires carriers to “isolate” the communications of the targeted customer and only then to deliver those isolated communications to law enforcement. If the provider has isolated the communications to law enforcement, then there is no need for law enforcement to use its own device or solution.

Privacy advocates may still regard CALEA as a threat to privacy. But CALEA itself does nothing to authorize intrusions into our private lives. The statute only gives Law Enforcement the technical capability to conduct surveillance when it is already authorized under other statutes. Surveillance authority and surveillance capability must go hand-in-hand. After all, what sense does it make to give an officer the authority to investigate a suspect without giving the officer the capability to do so?

Those are the seven myths surrounding the CALEA petition for rulemaking. I hope I have helped to dispel them. The purpose of the petition is clearly not to constrain the Internet, or harm the deployment of broadband communication services, or invade privacy. If successful, the petition would do nothing more or less than give Law Enforcement the CALEA tools it needs to carry out its mission in the broadband age.



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-11-2008 BY 60322/UCLRP/PJ/EHL

March 26, 2004

Privileged and Confidential
Protected by Attorney Client Privilege
Protected by Work Product Doctrine

MEMORANDUM

TO: Kerry Haynes, Assistant Director

FR: CALEA Implementation Unit Chief

b6
b7C

CC: Michael Clifford, Electronic Surveillance Technology Section Chief

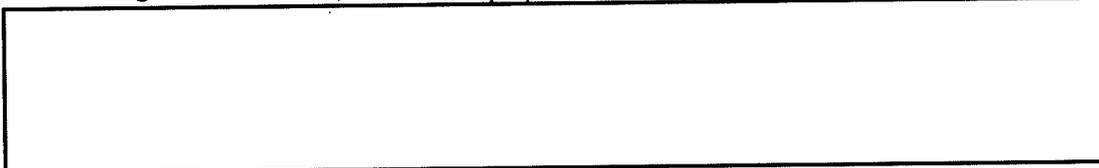
DA: March 26, 2004

RE: CALEA Legislative Initiative

CIU requests your review and approval of the attached CALEA Policy Position to formalize the FBI's position on the CALEA legislative initiative. Once the FBI's position is formalized, CIU will immediately coordinate with the Department of Justice, the Drug Enforcement Administration, and other Law Enforcement agencies to seek the needed legislative reform. The following explains the need for the CALEA Policy Position and addresses various related concerns.

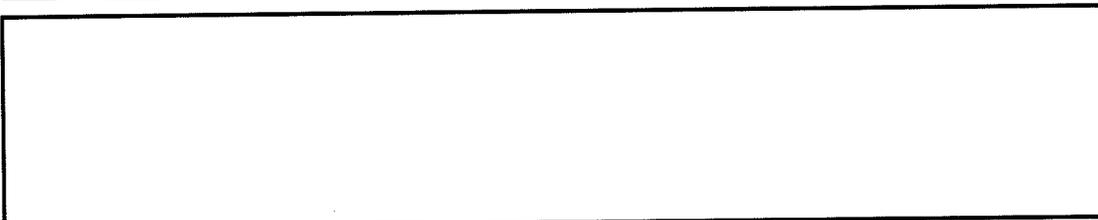
I. INTRODUCTION

The most important task faced by the CALEA Implementation Unit ("CIU") today is the CALEA legislative initiative, which is a proposal for Congress to revise the CALEA statute



A formal decision on the legislative matter is long overdue. As you know, certain congressmen have already commenced their own legislative initiatives on CALEA and the broadband industry. Three related congressional committees have made inquiries to solicit the FBI's views in their hearing proceedings. In addition, the 9/11 Commission has asked the FBI for input on electronic surveillance issues in preparation for the Commission's upcoming report on Homeland Security needs.

b2
b5
b7E



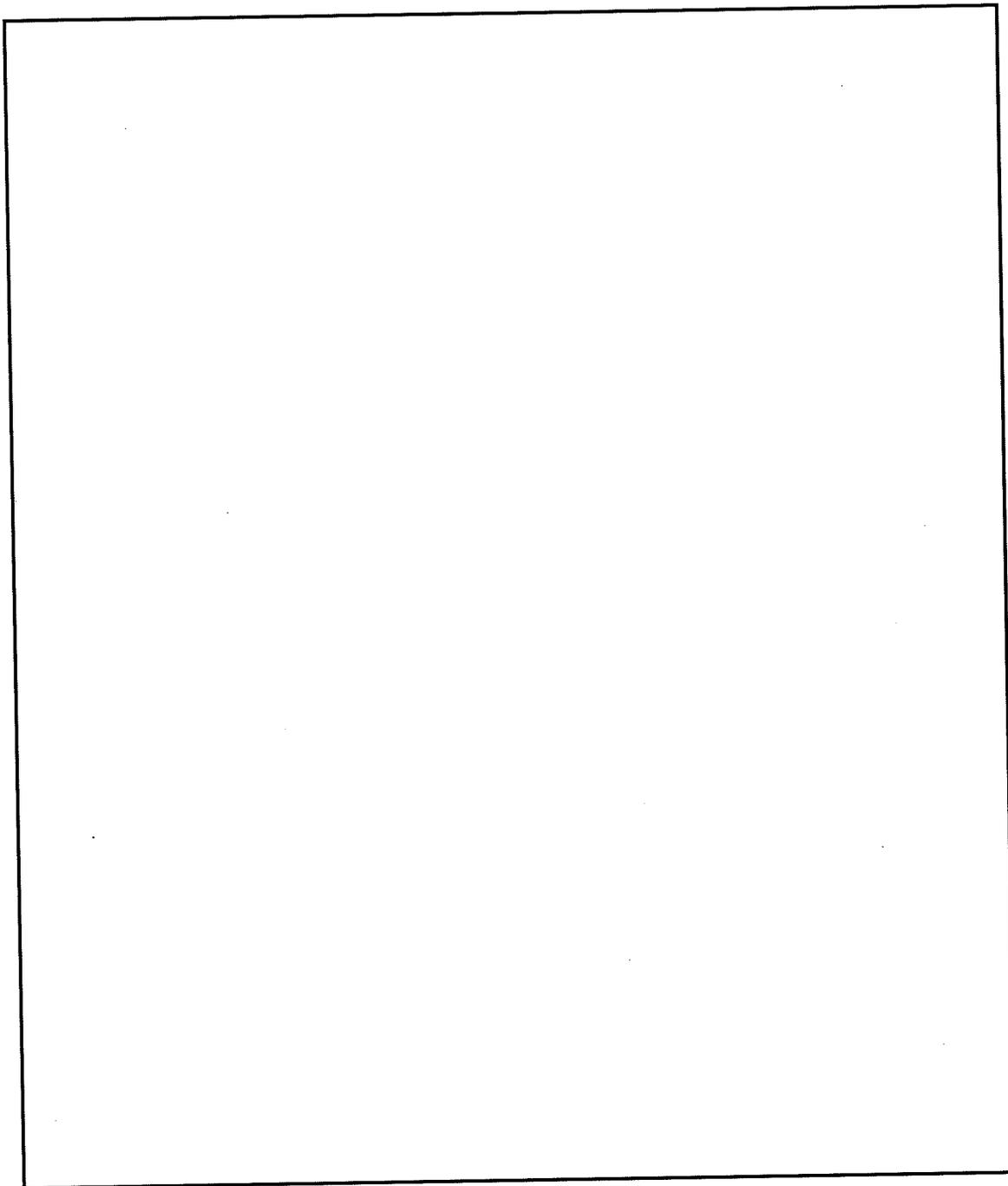
Federal Bureau of Investigation

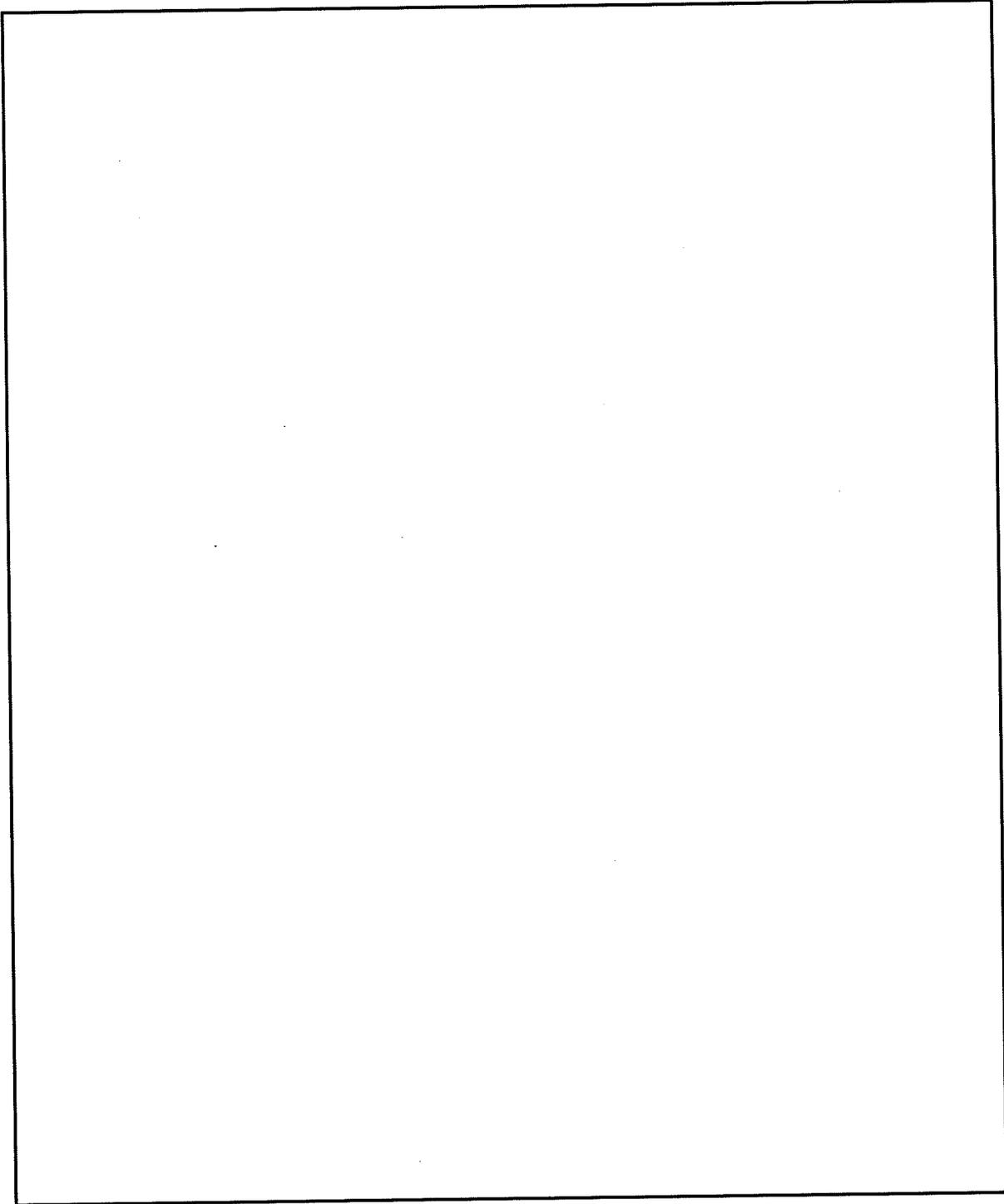
CALEALegislation: 040322mlegislative

RESPONSE to QUESTIONS

This document contains answers to questions asked by regarding
 Each question is reproduced and followed by its answer.

b2
b7E





b2
b7E

4. With regard to VoIP (SIP, H323, etc), are these IP protocols handled differently than the general case of IP communications for the following specific cases:
 - a. If the Telecom Provider Provides the VoIP as a managed service (e.g. Push to talk on the subscribers cell phone)

[Redacted]

- b. If the telecom provider does not provide VoIP service, but the intercept subject uses a VoIP service (e.g. SKYPE), that the TSP is not aware of.

Answer4b: Once again, J-STD-025B does not address packet-based voice communications. (A major reason that call content was renamed communications content in the standard.) [Redacted]

[Redacted]

[Redacted]

Category	Type	Problem Description	Enforcement of Existing Law	Legislation	Industry Liaison	LE Cooperation	Third Party Services	ELSR Technology	Standards	Additional Resources
IP Telephony	DSL derived Voice		Title 18 Action: "Show Cause" Timeframe: Ad hoc Title 50 Action: Timeframe: Ad hoc CALEA (no current CALEA-based capabilities) Action: Enforcement Timeframe: Ad hoc Regulatory Action: FCC enforcement	NA - current legislation accounts for service provider provision of access	Action: Industry Outreach Timeframe: (Input required)	N/A	N/A			Personnel Action: Non-personnel Action:
	WiFi Hotspots		Title 18 Action: "Show Cause" Timeframe: Ad hoc Title 50 Action: Timeframe: Ad hoc CALEA (no current CALEA-based capabilities) Action: Enforcement Timeframe: Ad hoc Regulatory Action: FCC enforcement		Action: Industry Outreach Timeframe: (Input required)					Personnel Action: Non-personnel Action:
	Facilities-based (e.g. broadband provider)		Title 18 Action: "Show Cause" Timeframe: Ad hoc Title 50 Action: Timeframe: Ad hoc CALEA (no current CALEA-based capabilities) Action: Enforcement Timeframe: Ad hoc Regulatory Action: FCC enforcement	NA - current legislation accounts for service provider provision of access (based on recent FCC NPRM)	Action: Industry Outreach Timeframe: (Input required)					Personnel Action: Non-personnel Action: b2 b7E
	Mediated (e.g. Vonage)		Title 18 Action: "Show Cause" Timeframe: Ad hoc Title 50 Action: Timeframe: Ad hoc CALEA (no current CALEA-based capabilities) Action: Enforcement Timeframe: Ad hoc Regulatory Action: FCC enforcement	NA - current legislation accounts for service provider provision of access (based on recent FCC NPRM)	Action: Industry Outreach Timeframe: (Input required)	N/A				Personnel Action: Non-personnel Action:
	Unmediated (e.g. [redacted])		Title 18 Action: "Show Cause" Timeframe: Ad hoc Title 50 Action: Timeframe: Ad hoc CALEA (no current CALEA-based capabilities) Action: Enforcement Timeframe: Ad hoc Regulatory Action: FCC enforcement	Action: assess viability of new legislation mandating either greater cooperation or specific capabilities (recent FCC ruling classify as information service) Timeframe: immediate	Action: Industry Outreach Timeframe: (Input required)	N/A	N/A	N/A		Personnel Action: Non-personnel Action:
Applications	[redacted]		Title 18 Action: "Show Cause" Timeframe: Ad hoc Title 50 Action: Timeframe: Ad hoc CALEA Action: NA	Action: assess viability of new legislation mandating either greater cooperation or specific capabilities (recent FCC ruling classify as information service) Timeframe: immediate	Action: Industry Outreach Timeframe: (Input required)			N/A		Personnel Action: Non-personnel Action: b2 b7E
	Software-based encryption (e.g. [redacted])				Action: Industry Outreach Timeframe: (Input required)			N/A		Personnel Action: Non-personnel Action:
	Bundled encryption (e.g. SSL, HTTPS)				Action: Industry Outreach Timeframe: (Input required)			N/A		Personnel Action: Non-personnel Action:
Protocol Processing								N/A		Personnel Action: Non-personnel Action:
Limitations of Law					Action: Industry Outreach Timeframe: (Input required)					Personnel Action: Non-personnel Action:

~~SECRET~~

b6
b7C

[Redacted] (OTD) (CON)

From: [Redacted] (CyD) (CON) b2
Sent: Thursday, September 28, 2006 3:07 PM b6
To: [Redacted] (CyD) (FBI) b7C
Cc: [Redacted] (CyD) (CON) b7E
Subject: [Redacted]

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b1
b2
b6
b7C
b7E

(S) FYI, the [Redacted]
[Redacted] (S)

[Redacted] Looks like the Bureau is on it's own with this one.

Moving forward, we've identified some next steps:

(S) [Redacted]

b1
b2
b7E

[Redacted]
[Redacted] b6
Special Projects Unit/STAO b7C
[Redacted] (Desk)
[Redacted] (STE)

DATE: 12-17-2008
CLASSIFIED BY 60322LP/plj
REASON: 1.4 (c)
DECLASSIFY ON: 12-17-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

Date: 04/12/06

To: [redacted] (Unit Chief)

From: [redacted] (CACI, Inc.)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-10-2008 BY 60322/UCLRP/PJ/EHL

b6
b7C

CC: [redacted] (DEA)

Subject: CTIA Wireless 2006

Participants: Wireless carriers and equipment manufacturers.

Synopsis: The Federal Bureau of Investigation's (FBI) Communications Assistance for Law Enforcement Act (CALEA) Implementation Unit (CIU) attended CTIA Wireless 2006 Exhibits that was held in Las Vegas, NV from 04/05/2006 thru 04/07/2006. The main purpose for the CIU participation was to:

[redacted]

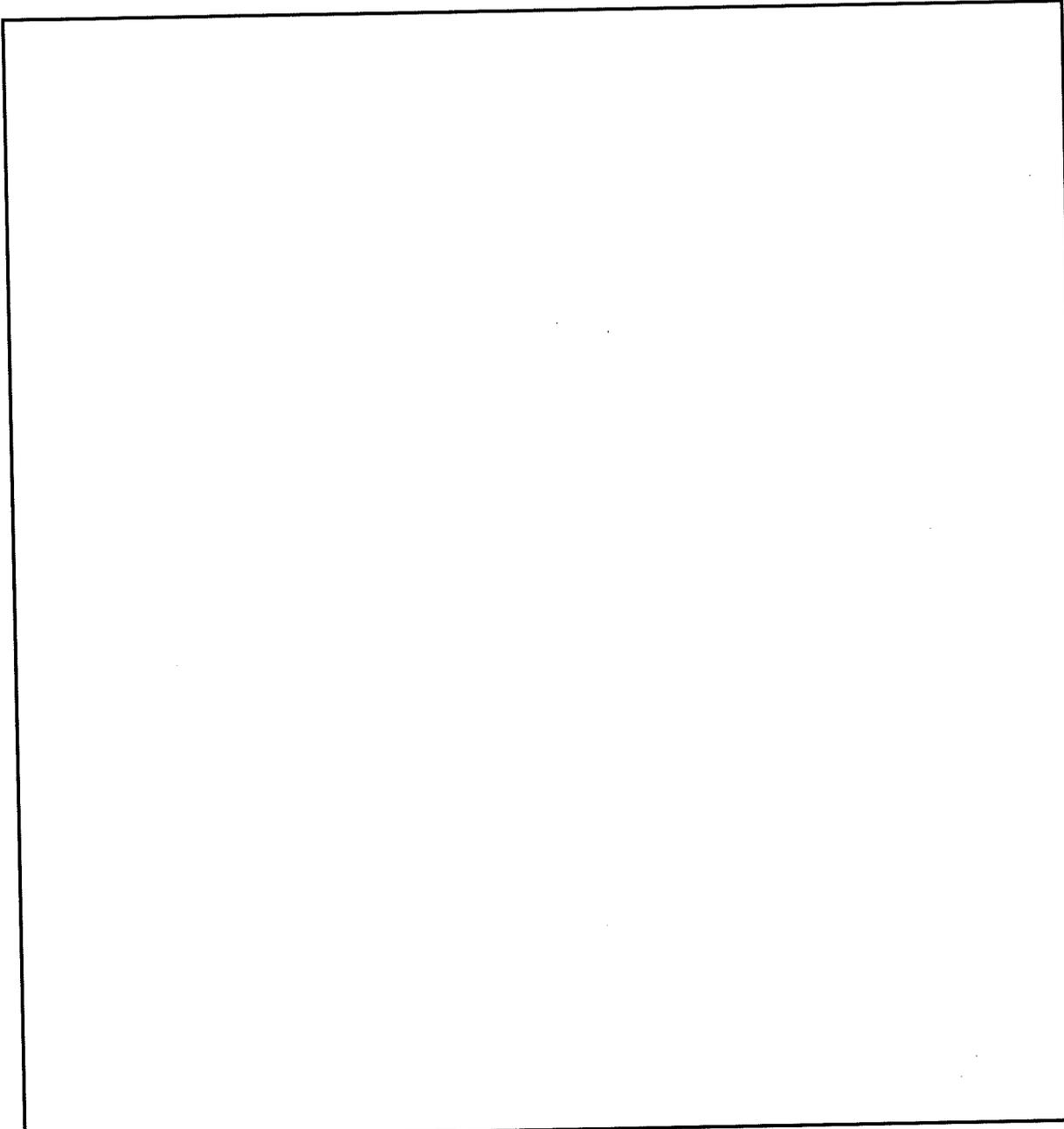
b2
b7E

Details: [redacted]

[redacted]

CIU DRAFT INPUT

*** FOR OFFICIAL USE ONLY ***



There are more than 100 products that have been Skype-certified. Netgear promotes its Skype Wi-Fi phone and Philips electronics also promotes its dual function phone with Skype

*** FOR OFFICIAL USE ONLY ***

CIU DRAFT INPUT

CIU DRAFT INPUT

*** FOR OFFICIAL USE ONLY ***

capability. There are several other manufactures with Skype built-in capabilities including Linksys, Aliph, Motorola, RTX, Logitech, and Sennheiser Communications.

*** FOR OFFICIAL USE ONLY ***

CIU DRAFT INPUT

August ETR Bulletin

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-10-2008 BY 60322/UC/LP/BJ/ZLL

- **Mobile Virtual Private Networks**
- **Mobile Ad Hoc Networks**
- **Cellular Network Signaling Security and Encryption**
- **Dynamic Spectrum Allocation**
- **Ringtones**
- **Inflight Communications**
- **Podcasting**
- **Mobile Virtual Network Operators – Summary**
- **ENUM**
- **Optical Networks**
 - **IP – Private Branch Exchange (IP PBX)**
 - **Steganography Steganography and Digital Watermarking**
 - **Location Based Services**
 - **Finding Service Provider Information**
 - **Skype Update – Cordless DECT Phones**
 - **From the Field: SAC Brinkman**
 - **VoIP 10 Tutorial**
 - **Service Provider Highlight: TomatoVine™**

For Official Use Only

FBI – Electronic Surveillance Technology Section

Example: Net-2-Phone / Skype etc.

- Using Pier-2-Pier & Managed VoIP Service
 - Free or Pre-Paid Services
 - **Off Short Service Reseller**
 - **Non Traceable Payment Plan**

For Official Use Only

FBI - Electronic Surveillance Technology Section

Subject Identification:

Access Points:

ELSUR

Processing:

Complete Information:

- Pier-to-Pier Services
- TomatoVine™
- Skype™
- SpyderNet™
- AOL VoIP
- In-Flight Broadband Service
- AirCell
- LiveTV (Jet Blue)

Accurate Information:

b2
b7E

1.1 Highlights of Convergence

Tutorial discussing the history and future direction of communications technologies

1.2 Voice over IP

Discussion of Voice over IP (VoIP) technology

1.3 Service Provider Highlight- AT&T CallVantageSM

AT&T service offering for Voice over IP (VoIP) service through Broadband cable access

1.4 WiFi Hotspots

Discussion of Wireless Fidelity (WiFi) Hotspot technology

1.5 P2P IP Services- Internet Telephony and Online Gaming

P2P Internet services are discussed. Services include Skype, Session Initiation Protocol (SIP) phones and online gaming

1.6 Unregistered Phone Pay-Per-Call Mobile Service

Service allowing deactivated phone to be used in the network

Two new i-name digital address namespaces become available: "=name" and "@name." Individuals may use their =name as a privacy protecting alternative to giving out email addresses or telephone numbers. For example, individuals may freely publish their =name as their public contact point on web-pages, blogs, or business cards as a way to be contacted by others who can also authenticate their digital identity which prevents spam. Businesses, organizations or other groups may use their @name to offer a variety of new digital identity and trusted data exchange services. I-names, which are based on the XRI (Extensible Resource Identifier) specifications from OASIS, may initially be registered in English, Latin, Chinese, Japanese, and Korean characters. Support for additional character sets is planned for the future.

In addition to spam safe contact service, i-brokers will be offering two other basic i-services: single sign-on service, which enables consumers to use their i-name and a single, strong, secure password to log in to websites or web based applications; and forwarding service, which allows individuals or businesses to create their own simple, permanent digital addresses for web-pages, blogs, photos, videos, files, etc.

Links to all participating i-brokers, and further information about i-services are available at <http://www.inames.net>.

16. SKYPE UPDATE: CORDLESS DUAL PHONE

Skype has impacted the telecommunications industry and continues to interest customers with new and constantly improving services. The industry marketplace waits for the emergence of GSM/WiFi dual mode handsets that were introduced at several international telecommunications conferences in 2005 and 2006.

The dual mode phone that is already available is the cordless DUAL phone, which is a Digital Enhanced Cordless Telephone (DECT), that can be connected to a phone socket and a USB port on a PC. Using the Skype service, the user can make unlimited Skype calls to other Skype users or utilize the SkypeIn and

SkypeOut services, which allows users to access the PSTN.

The DECT phone handset shows the user which Skype contacts are available and also provides call forwarding, call waiting, and caller ID (requires service from your telephone operator).

In order to start using Skype on the DUAL phone, the user must install the Skype software (the Skype CD is included with the DUAL phone) on to a PC. Once it is installed the user will plug the DUAL phone into the USB port on the PC, and the Skype software will update the phone and provide all necessary user information including contact lists.

What is DECT?

DECT is the European digital standard for portable, wireless phones to the telecommunications network. DECT phones are similar to the GSM cellular system in that they both use Time Division Multiple Access (TDMA), but the cell radius is only about 25-100 meters whereas GSM cells are range from 2-10 kilometers. DECT works optimally for a smaller areas with a larger number of users.

Part of the DECT standard describes how it interacts with the GSM standard so users can be move between the outdoors (and GSM signals) into an indoor environment (and a DECT system). The telecommunications industry anticipates that many GSM service providers will extend their service to support DECT signals inside buildings. A dual-mode phone would automatically search first for a DECT connection, then for a GSM connection if DECT is not available.



[redacted] (OTD) (CON) b6 b7C

From: [redacted]
Sent: Thursday, January 11, 2007 9:30 AM
To: [redacted]

b6
b7C

Subject: iSkoot "a New mobile killer application model"

[redacted]

iSkoot, the service provider for mobile Internet (based in Cambridge, MA) announced this week that the iSkoot proprietary client software and its API has been Skype certified and it is available as free download software that can easily be integrated into most new mobile phones. This announcement confirms that iSkoot client software meets both mobile environment and Skype standards for usability and quality on the existing wireless networks. With iSkoot, VOIP users can take advantage of Internet phone services and buddy system to make unlimited VOIP calls using their P2P software from their cell phone.

This capability, when implemented in the mobile phones, allow users to make Skype calls (as well as other Skype services) on standard wireless networks. The iSkoot client software allows mobile users to place and receive Skype calls from their handsets, without the need for special hardware/software, PC or Wi-Fi/WiMAX or broadband Internet networks. [redacted] b2 b7E

According to iSkoot-Skype, the iSkoot client software currently supports Motorola Razor phones and Symbian-based mobile phones. Current MS models supported are:

- Motorola (RAZR V3, SLVR L7, PEBL, v557)
- Nokia (6021, 6102, 6600, 6680, 6682, 6030)
- Sony Ericsson (v600i, w600i)

iSkoot also plans to support other Internet Protocol based services including Chat, IM, Google talk, Yahoo Messenger, and PC-based calling platforms.

It is estimated that there are more than 136 million Skype PC based users worldwide using Skype PC client software for IP services. The iSkoot Skype wireless solution, when implementation could easily double the number of Skype wireless users in a very short time taking advantage of Skype features and "free" wireless services.

The iSkoot Skype API could be the next killer application in mobile environment!

Should you have any questions please call me

[redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-10-2008 BY 60322/UCLRP/PJ/EHL

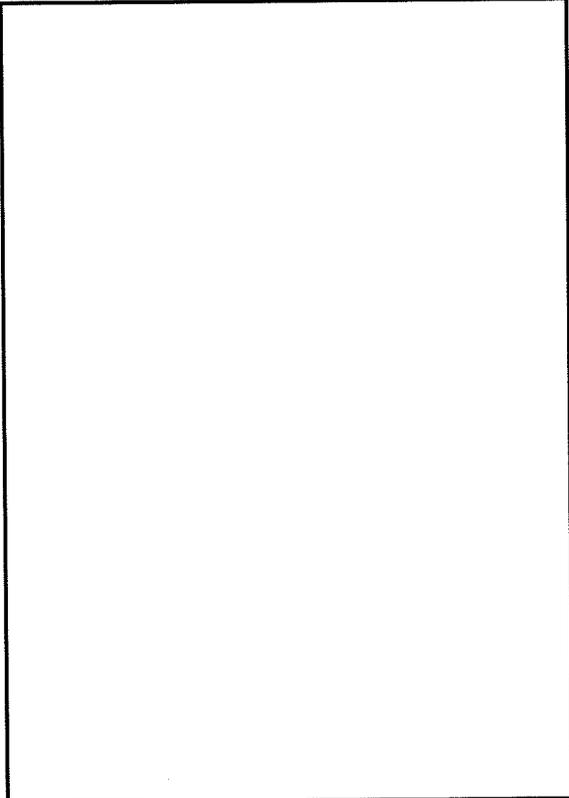
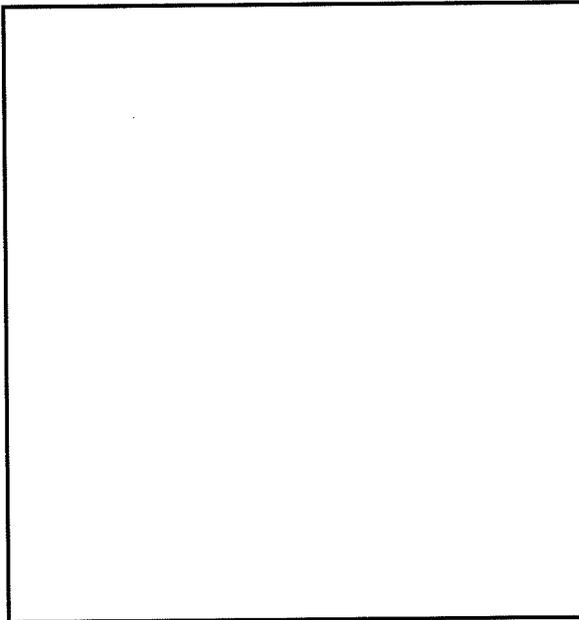
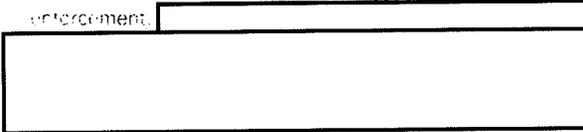
4/11/2008

Executive Summary

Voice over Internet Protocol (VoIP) affords users the ability to make telephone calls over a data network such as the internet. VoIP converts the voice signal from a telephone or headset into digitized packets tagged with source and destination addresses. These packets then travel across the internet. At their destination, the packets are reassembled, and the digital signal is converted back to a voice representation. This process enables the user to speak to anyone with a traditional phone or a computer. When traversing the network, the packets take the most efficient route based on network equipment's application of services and policies, to improve throughput delay.

VoIP is gaining popularity as an alternative to traditional telephone service, as illustrated by traditional telephone companies' introduction of their own VoIP services. These new services include AT&T's CallVantageSM and Verizon's VoiceWingsSM.

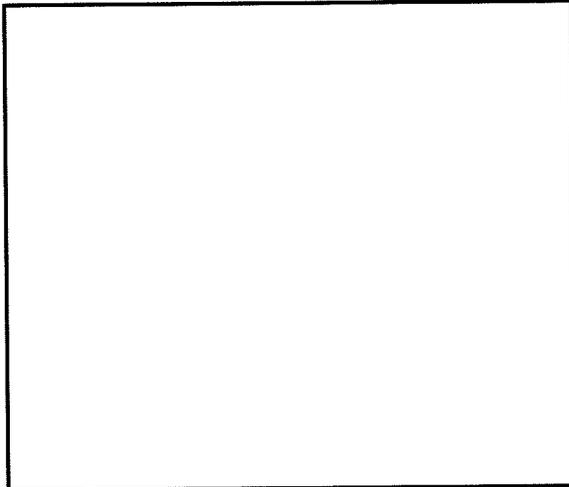
Like other popular technologies or services (e.g., the internet and computer-based services), VoIP presents an attractive target to attackers interested in disrupting service. This article discusses some of the known threats to VoIP service and some additional VoIP issues relevant to law enforcement.



b2
b7E

Law Enforcement Issues

Some vulnerabilities of VoIP may have particular impacts on law enforcement.



1. See, e.g., <http://www.fbi.gov/newsroom/stories/2008/08/080808a.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808b.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808c.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808d.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808e.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808f.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808g.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808h.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808i.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808j.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808k.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808l.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808m.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808n.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808o.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808p.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808q.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808r.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808s.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808t.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808u.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808v.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808w.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808x.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808y.htm> (discussing the use of VoIP in a terrorist attack); <http://www.fbi.gov/newsroom/stories/2008/08/080808z.htm> (discussing the use of VoIP in a terrorist attack).

confidentiality, replay protection and non-repudiation), infrastructure to support MIP, VPN and Authentication Authorization and Accounting (AAA) between the mobile client and the intended trusted network and finally the smarts or intelligence required within the mobile unit to know when to invoke VPN security when the mobile communicates from an untrusted network. The figure shows the migration of mobile devices across technological medium boundaries as scenarios with the endgame being the continuous communication with the enterprise intranet. As would be expected the final solution to implementing Secure Seamless Mobility (SSM) will not come all at once due to the complexity of the wireless and Internet protocols and infrastructure as well as their interoperability. What is expected though is a piece meal approach to providing Seamless Mobility at first in business markets, later incorporating the residential markets and finally the complete package incorporating security and reigning in the consumer and financial markets.

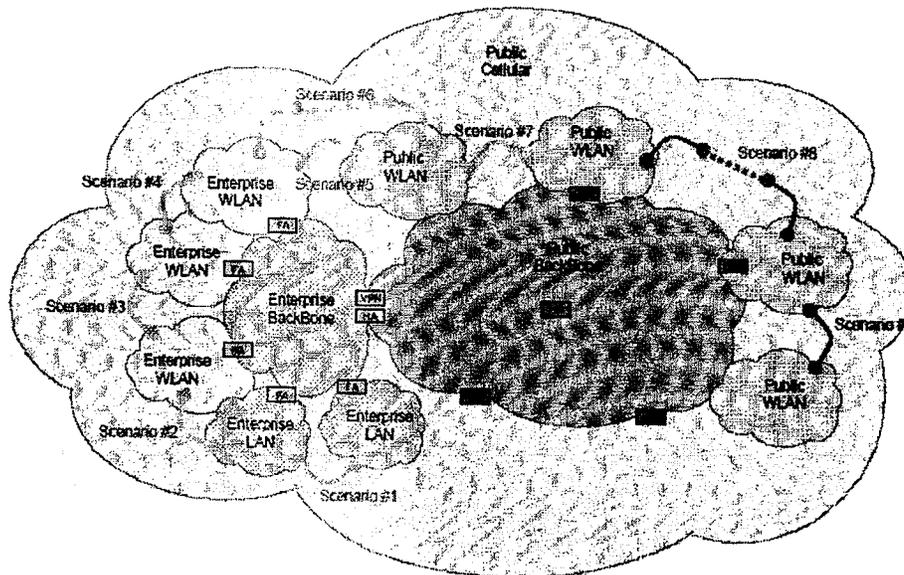


Figure 1:

A new breed of mobiles are entering the consumer market allowing access to both cellular and WiFi technologies.³ As predicted by the previous bulletin's article on MultiNetwork Mobile Devices, "the advent of third-party voice service, subjects using PDA-type devices can communicate outside the traditional cellular channels by using the cellular and WiFi services as a simple data bearer service for voice application", has become a reality as stated in LongDistanceWorld.com.

"Motorola, Inc., a global leader in seamless mobility, and Skype Technologies S.A., the Global Internet Telephony Company(TM), announced their intention to work together on a co-marketing collaboration that will provide greater connectivity options and access for Skype's more than 25 million registered worldwide users. The alliance will explore opportunities broadly across both companies, leveraging Motorola's strength in seamless mobility, advanced technologies, mobile devices and accessories and Skype's rapidly-growing global user base and rich voice and messaging communication tools. The initial focus of the collaboration will be on co-marketing of new optimized Motorola 'Skype Ready' companion products, such as Bluetooth(R) headsets, dongles, and speakerphones, as well as delivery of the Skype Internet Telephony experience on select Motorola mobile devices. "By making Voice over IP truly mobile and easily accessible, we can make communications seamless for consumers as they travel throughout the environments of their day - at work, at home, in the car, or out in the world," said Liz Altman, vice president of business development, Motorola Mobile Devices. "With over 68 million downloads of their

³ See "MultiNetwork Mobile Devices," ETR Bulletin, Volume 2, Issue 1 (January 2005).

client in the last 18 months, we believe Skype is a natural fit with our vision of simple and seamless connectivity for our consumer customers around the globe." Skype takes communications to a new and global era with its free, multi-faceted and rich communication tools, enabling users to make free voice calls and rich messaging connections via the Internet. Skype is the leading VoIP-category product worldwide, with more than 25 million registered users."⁴

With multiple network access from one mobile device, the ability to allow roaming internet hosts to maintain constant IP address and uninterrupted IP-level connectivity back to a home network while changing points of attachment to a network and network access technology has been established using the MIP protocol. MIP was adopted by cellular systems such as Motorola iDEN deployed by Nextel and more recently by cdma2000 standards for core networks, and for these systems, it evolved to take into account the needs of commercial environments. Today Mobile IP is being increasingly considered a preferred method for support of multi-access technologies and inter-system roaming.⁵

So far, the mobile device allows access to different networks and MIP provides a method for arriving at the restricted/private home network. Securing the channel or session between the mobile user and the home network is accomplished by the VPN and IPsec protocols. Simply put, a VPN is a network that provides authentication, confidentiality, and private communications over an untrusted medium. With IP, there is no guarantee that the packet is from the expected sender and the data contained is what was transmitted. Even if these two are not considered, there is no assurance that the contents have remained private and not been disseminated. IPsec was created to thwart these vulnerabilities by providing several layers of protection with authentication, encryption, message authentication, and the leveraging of existing security concepts applied in combination to the communication. IPsec is defined by several Internet Engineering Task Force (IETF) Request For Comments (RFCs) that detail the many layers of the technology. IPsec provides for three primary types of communication, client-to-network, network-to-network and client-to-client. In other words, communications can be secured between the mobile user and the home network, between a home network and a business network as well as between a mobile user and another mobile user.⁶ An example of a secured VoIP communications network (i.e., the network-to-network model) using IP-PBX at different regional locations can be seen in the previous bulletin discussing VoIP updates.⁷

Bringing all the key components together to create a Secure Seamless Mobility feature, requires the support of edge networks (e.g., Cellular Service Providers and WiFi Service Providers) passing mobile information onto the Internet and allowing access back to the mobile client in the form of IP packets. The mobile device will provide MIP and VPN protocol support to communicate end-to-end with the home network as well as network routers/servers in visiting networks which relay communications onto the home network.

Implementation:

A Seamless VPN system will allow seamless mobility across security boundaries between the Internet and the Intranet of a business or residence. A secure boundary is created by the use of a standardized IETF component called the Home Agent is deployed on the external DeMilitarized Zone (DMZ), a buffer to the official Internet world via private addressing, and synchronized with the main Home Agent which is placed securely on the enterprise Intranet. The key to this implementation is to establish two separate Mobile IP systems. Both mobility systems can be handled from a single client process located on the mobile device and communicating with its peer Mobile IP Home Agents, shown in Figure 2. Both mobility systems

⁴ Motorola, Inc., "Motorola and Skype Form Broad Seamless Mobility Alliance", LongDistanceWorld.com, February 14, 2005.

⁵ Alex Shneyderman and Alessio Casati, "Mobile VPN, Delivering Advanced Services in Next Generation Wireless Systems", Wiley Publishing, Inc., 2003.

⁶ James S. Tiller, "A Technical Guide to IPsec Virtual Private Networks", CRC Press LLC, 2001.

⁷ See "VoIP Updates," ETR Bulletin, Volume 2, Issue 1 (January 2005).

- The internal (HA on intranet) Mobile IP system mobilizes your application (using the advantages of the method described in Mobile IP inside VPN model).
- The external (HA on DMZ) Mobile IP system mobilizes your VPN (using the advantages of the method described in the VPN overlaid Mobile IP model)

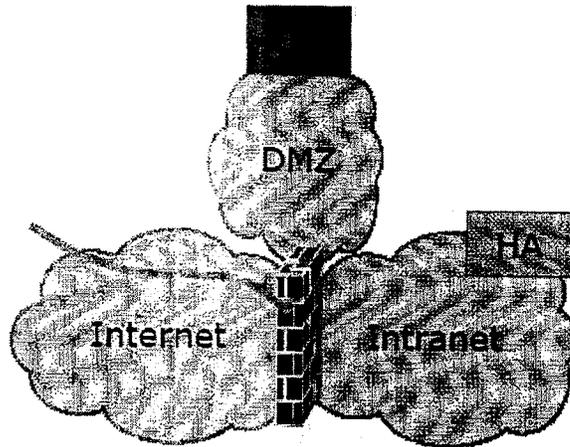


Figure 2: Separate Mobile IP Systems

Figure 3 shows the sequence needed for your client to connect from the outside to the enterprise network when using the Mobile IP implementation. As shown in the figure there is an increased complexity of the communication that needs to take place between all the components involved to be able to reach the enterprise from the outside.

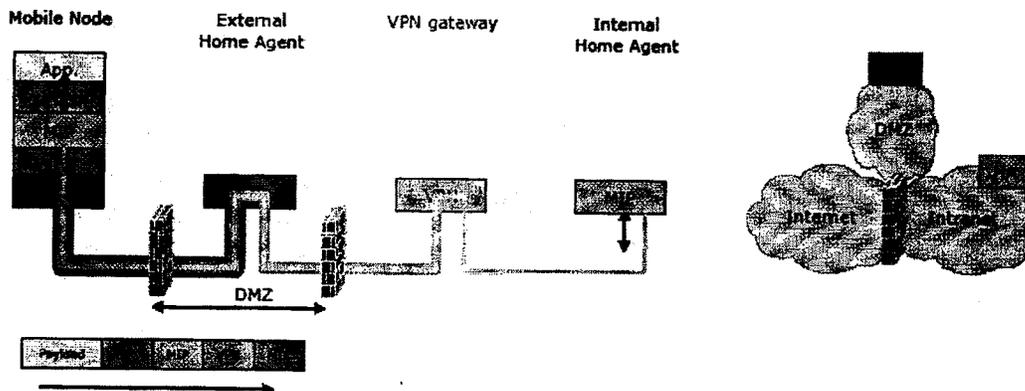


Figure 3: Access to the Intranet from outside the Internet

Figure 4 shows the sequence needed for a client to connect to the enterprise network when using the Mobile IP implementation and the client is on the inside. This case is a simpler case compared to reaching the enterprise network from the outside. The VPN client becomes inactive and the VPN overhead is not incurred for internal communication.

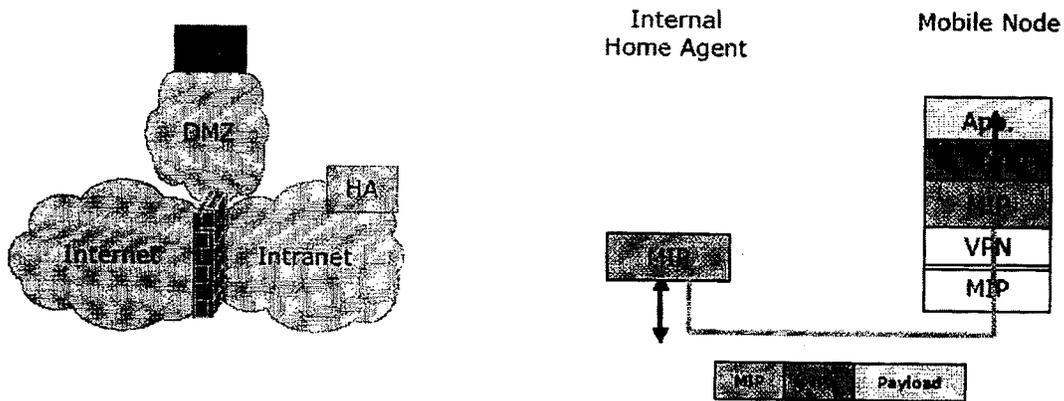


Figure 4: Access to the Intranet from inside Intranet

This implementation of Secure Seamless Mobility solves the key issue of mobilizing your standard VPN solution while turning it on only when the user is connecting from an external insecure network. In this way, the load on the VPN concentrators and the Firewall network components are kept as low as possible. Users are able to move seamlessly both between different internal networks, between different external access networks, and across the security boundary protected by VPN and Firewall technologies. The VPN is turned on or off as required. VPN is turned off when public networks are used, and VPN is turned on only on existing standard-based components such as industry standard VPN components, industry standard Mobile IP Home Agents together with the IETF-standard based Mobile IP client. Using this architecture, you can rely on well-proven network components, and do not need any proprietary signaling between any of the components in the solution. Further more, large-scale deployment of Mobile IP is now possible using the standard-based web infrastructure of the operator or enterprise to automatically configure the client with no manual configuration steps needed by the end user. This feature enables the organization to quickly introduce seamless and secure mobility for their existing user base, without extra technical requirements to the end user.⁸

Service Providers:

Motorola

Using 802.11 technology inside the enterprise and cellular telephony elsewhere, the solution supports contiguous communications across networks. Now, the office phone is no longer tethered to the desk. Now, key IP PBX-based features are available on the road. And now, each team member can be more effective with only one phone number, one voice mail to manage and access to corporate data available both inside and out of the office. It's a total business solution designed around your enterprise.⁹

Tekelec

Businesses today are challenged to support workers in many locations with a variety of communication requirements while containing costs. With the fixed and mobile VPN solutions, service providers are able to help enterprise customers connect offices in multiple locations and support workers in multiple locations.¹⁰

ipUnplugged

⁸ "Seamless Secure Mobility Across All Networks White Paper", Birdstep Technology ASA, 2002.

⁹ <http://www.motorola.com/wlan/index.html>

¹⁰ http://www.tekelec.com/solutions/s_detail.asp?id=31

ipUnplugged is the leading developer of Network Services software for seamless and secure roaming across public and enterprise LANs, WLANs, GPRS, CDMA, and 3G networks. ipUnplugged's Roaming Client, Roaming Gateway, and Roaming Server software enables users to roam securely and seamlessly from one network to another without having to reconnect, change settings, or lose connectivity at any point in time. The products are based upon industry standards and technology including Mobile IP, IPsec, and standard AAA. The ipUnplugged solution is used both by mobile operators and enterprises.¹¹

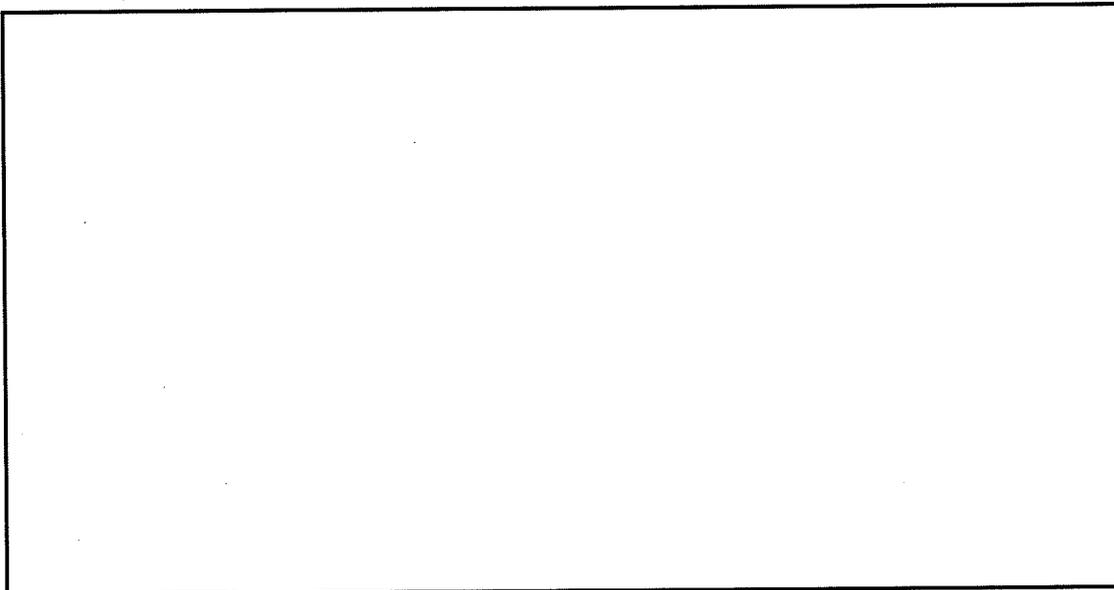
Birdstep

Switching between Ethernet, cell-phone, wireless LAN and Bluetooth connectivity requires in-depth knowledge of numerous setup parameters. Furthermore, yesterday's technology did not provide for uninterrupted connectivity as the user switched networks, e.g. unplugged the computer from the Ethernet in the office and switched to the WLAN. Mobile users now demand hassle-free configuration and seamless handover between various networks. Birdstep Technology delivers software solutions to address these market requirements.¹²

Avaya

Avaya, Motorola and Proxim have collaborated to deliver the first truly integrated, seamless mobile voice communications solution. Available in the fourth quarter 2004, the solution includes a dual network Modular Office Device (MOD) from Motorola that functions as a fully-featured extension of Avaya Communication Manager. Seamless voice communications can be supported on the 802.11 wireless network within an office building, on the cellular network while workers are on the go, and while roaming between the two. Key associates and executives can have the functionality of their Avaya desk telephone on a mobile handheld device without using cellular minutes inside the building.¹³

Impact Summary:



b2
b7E

¹¹ <http://www.ipunplugged.com/about.asp>

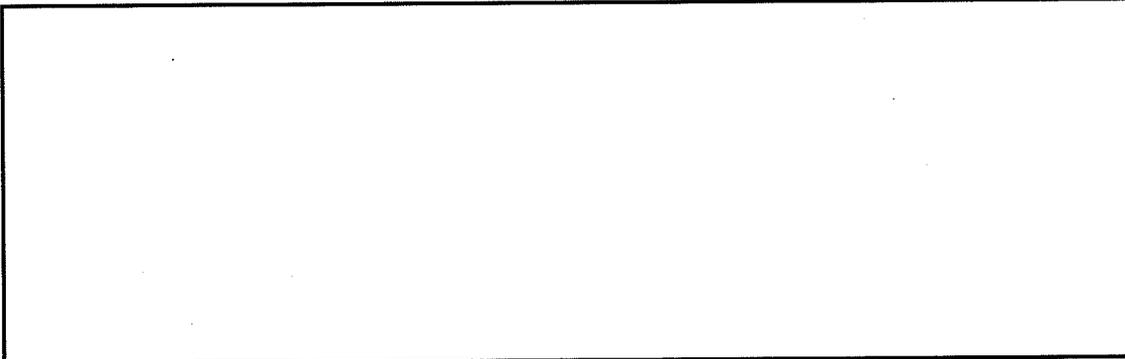
¹² http://www.birdstep.com/wireless_infrastructure/index.php3

¹³ http://www1.avaya.com/enterprise/whitepapers/map_solution.pdf

Executive Summary:

Mobile phones, Personal Data Assistants (PDAs) and laptops providing voice and data services are beginning to switch communication paths from cellular carriers' wireless networks to company Wireless Local Area Networks (WLANs) to Public Wireless Local Area Networks (PWLANS) (a.k.a. hot spots and hot zones) without service disruptions. The ability for mobile devices to support multiple connections across technology mediums represented by General Packet Radio Service (GPRS), Enhanced Data Rates for GPRS Evolution (EDGE), Third Generation Code Division Multiple Access 200 (3G cdma2000), Third Generation Universal Mobile Telecommunication System (3G UMTS), 801.11b/g, and Bluetooth will provide the foundation for supporting seamless mobility. Seamless mobility provides roaming from a mobile phone when outside the office or home to WLANs or PWLANs within the confines of a business or residence. The mobile user will have one mobile device with one number to communicate instead of pockets or purse full of communication devices. In addition, the mobile device will be smart enough to determine which wireless technology to use based on reliability, cost, bandwidth, quality of service and security. Seamless mobility provides the mobile user twenty-four by seven access to company, home and third party information and services.¹

The increase and proliferation of 3G wireless networks that support higher data rates and internet services such as Quality of Service (QoS), Multi-Protocol Label Switching (MPLS), firewalls, Internet Protocol (IP) filtering and Virtual Private Network (VPN) involving Internet Protocol Security (IPSec) will become the next increment in technology moving from seamless mobility to Mobile VPN (MVPN). Service providers of MVPN will provide secure mobile data networks over generally insecure shared mobile and wireless facilities as well as private mobile and wireless facilities. The service offerings to be provided by MVPN will be smart vending machines, information-collecting devices, utility metering, intelligent cash registers, highway toll stations, security systems, medical equipment, remote private access, and banking services.²



b2
b7E

Technology:

Overview:

In a nutshell, the ability to communicate across a diverse network seamlessly and securely, as depicted in Figure 1, requires the following: mobile devices capable of communicating over diverse technological mediums, the use of the Mobile IP (MIP) protocol enabling the ability to roam across large geographical areas while maintaining the same packet-data session with the same IP address, the invocation of VPN with IPSec providing the ability to send information in a secure manner (i.e., the sending and delivery mechanism of information is provided with connectionless integrity, data origin authentication,

¹ Kelly Unga, "The next step in mobility: Seamless wireless network roaming", Intermec Technologies Corporation, SearchMobileComputing.com, May 4, 2003.

² Alex Shneyderman and Alessio Casati, "Mobile VPN, Delivering Advanced Services in Next Generation Wireless Systems", Wiley Publishing, Inc., 2003.



**COMMUNICATIONS ASSISTANCE FOR LAW
ENFORCEMENT ACT (CALEA)**

Technical Standards

MOTIVATION FOR PARTICIPATION IN STANDARDS

Industry initiates and participates in the development of lawful intercept standards in order to be afforded the "Safe Harbor" provision of Section 107 of CALEA

A carrier shall be found in compliance with Section 103 of CALEA if the carrier has implemented the capabilities set forth in an industry accepted standard

Industry develops standards for interception with or without law enforcement involvement

Industry is highly motivated to develop standardized intercept solutions based on the general goals of open standards and the "Safe Harbor" provision of Section 107 of CALEA

FBI attendance provides end user perspective (i.e., the customer)

The FCC concluded in its Second Report and Order that absent the filing of a deficiency petition under CALEA section 107(b), it would be premature for the FCC to intervene in the standards development process

TODAY'S "AVERAGE" COMMUNICATIONS CUSTOMER

The average communications customer utilizes several services

- Residential voice service (traditional voice, "carrier grade" VoIP)

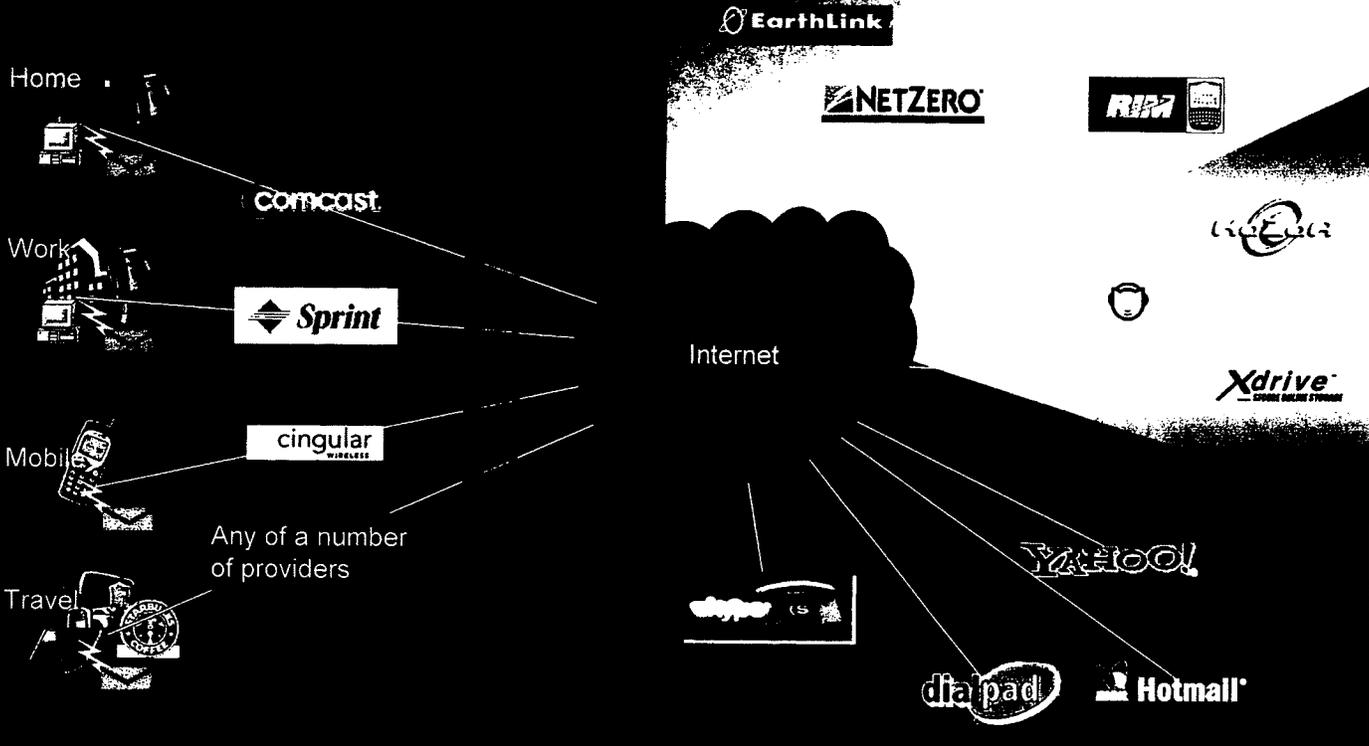
- Residential broadband access service (xDSL, Cable)

- Cellular voice and data service (GSM, CDMA)

- Open access wireless service (Starbucks, municipal Wi-Fi)

This allows for multiple access methods to a variety of services

MULTIPLE ACCESS METHODS TO A VARIETY OF SERVICES



ALWAYS ON, ALWAYS CONNECTED, ALWAYS MOVING WIRELESS SERVICES / CAPABILITIES



	<i>iPhone</i>	<i>Cingular 8525</i>	<i>Blackberry Curve</i>	<i>Samsung Blackjack</i>
<i>2.5G (GPRS)</i>	•••••	•••••	•••••	•••••
<i>3G (UMTS)</i>	•••••	•••••	•••••	•••••
<i>Wi-Fi</i>	•••••	•••••	•••••	•••••
<i>Bluetooth</i>	•••••	•••••	•••••	•••••
<i>GPS</i>	•••••	•••••	•••••	•••••
<i>3rd Party Applications</i>	•••••	•••••	•••••	•••••
<i>Keyboard</i>	•••••	•••••	•••••	•••••
<i>Touch Screen</i>	•••••	•••••	•••••	•••••
<i>Price (with contract)</i>	\$499.99	\$299.99	\$199.99	\$99.99

T Mobile

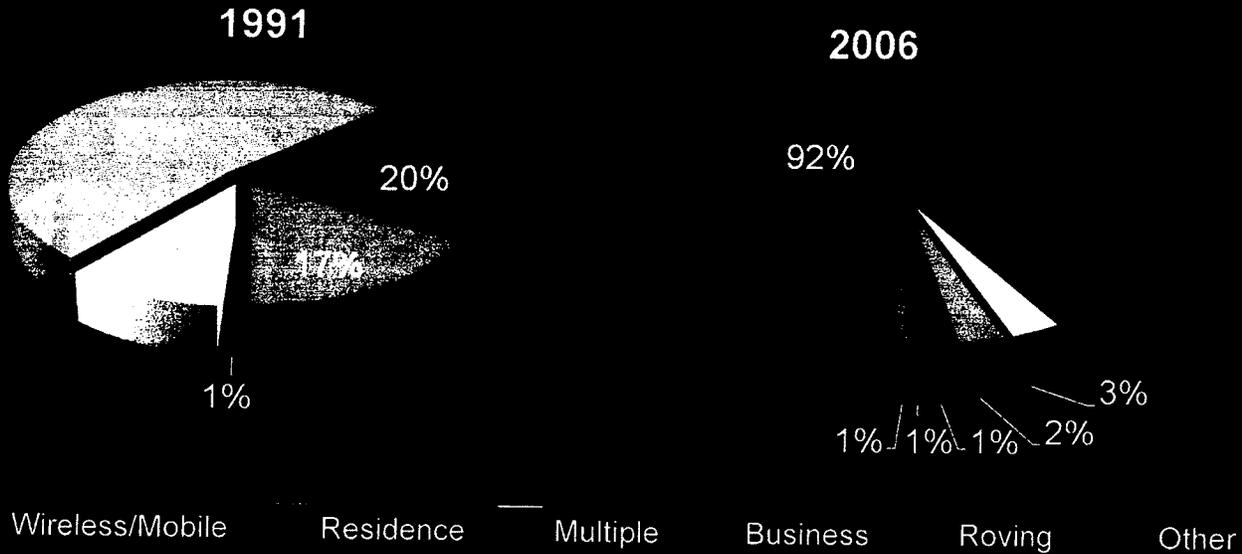


	<i>Blackberry 8800</i>	<i>Slickick</i>	<i>Blackberry Pearl</i>	<i>Dash</i>
<i>2.5G (GPRS)</i>	•••••	•••••	•••••	•••••
<i>3G (UMTS)</i>	•••••	•••••	•••••	T
<i>Wi-Fi</i>	•••••	•••••	•••••	•••••
<i>Bluetooth</i>	T	T	T	T
<i>GPS</i>	•••••	•••••	•••••	•••••
<i>3rd Party Applications</i>	T	T	T	T
<i>Camera</i>	•••••	•••••	•••••	•••••
<i>Keyboard</i>	T	T	T	T
<i>Touch Screen</i>	•••••	•••••	•••••	•••••
<i>Price (with contract)</i>	\$349.99	\$199.99	\$149.99	\$149.99

ELECTRONIC SURVEILLANCE TRENDS - WHERE TITLE III WIRETAP AUTHORIZATIONS OCCUR

Shift in location of wiretaps

Wireless / mobile technologies are the preferred medium of communications for targets



Source: 2006 Wiretap Report, Administrative Office of the United States Courts

QUESTIONS

[REDACTED]

Unit Chief

CALEA Implementation Unit
Operational Technology Division
Federal Bureau of Investigation

[REDACTED]

b6
b7C

b6
b7C

Message

1 of 4

[redacted] (OTD) (FBI) b6 b7C

From: [redacted] (CQ) (FBI)

Sent: Friday, April 22, 2005 1:47 PM

To: [redacted] (CyD) (FBI)

Cc: [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (ITD) (FBI); [redacted] (CQ) (FBI)

b6 b7C

Subject: RE: Intel Assessment for review

SBU

**SENSITIVE BUT UNCLASSIFIED
NON-RECORD**

b6 b7C

Comments on Skype Intel Assessment:

3 pages

General Comments:

[redacted]

[redacted]

b2 b7E

found
LES

[redacted] b7E

3. Cost is 2 cents/min

[redacted] b2 b7E

[redacted] b2 b7E

[redacted] b2 b7E

7. IMPORTANT: [redacted] b2 b7E

PG 1 1st bullet: [redacted]

pg 1 bullet 2: [redacted]

pg 2 top: [redacted] b2 b7E

pg 4 top: There have been 100 million software downloads, and a reported 7.8 billion minutes used. This indicates more than 100,000 users.

pg 5 1st bullet: 2 cents not .2 cents.

pg 6 MOTIVES: [redacted]

pg.7 Conclusion: Comment.. [redacted]

Please contact DICTU @ ERF for specifics on interception. UC [redacted] b6 b7C

6/19/2008

[Redacted]
OTD ATU

b6
b7C

-----Original Message-----

From: [Redacted] (CyD) (FBI)
Sent: Thursday, April 21, 2005 3:53 PM
To: [Redacted] (CQ) (FBI)
Subject: FW: Intel Assessment for review

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hi [Redacted]

b6
b7C

Cyber received the attached Assessment from the Office of Intelligence to review prior to its being published. I have looked it over and have some concerns with the piece. I spoke with [Redacted] and he thought that you would be a good person to also take a look at the Assessment. This was done by the San Diego field office and while I applaud their effort, I do have some concerns about a number of their statements.

b6
b7C

I have negotiated additional time from the OI and they granted me an additional week for the review. Any help you can give will be definitely appreciated.

Thanks so much!

[Redacted]
Supervisory Intelligence Analyst
CyD/CIAU

b6
b7C

-----Original Message-----

From: [Redacted] (OI) (FBI)
Sent: Tuesday, April 19, 2005 12:32 PM
To: [Redacted] (CyD) (FBI); [Redacted] (CyD) (FBI); [Redacted] (CyD) (FBI)
Subject: FW: Intel Assessment for review

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Hello All,

The attached assessment was submitted to SAPU by San Diego for review. SAPU personnel will provide guidance regarding format/scope/analytical soundness and editorial comments regarding grammar. CYBER is requested to review the product and provide substantive factual comments. SAPU will consolidate the comments and send guidance back to San Diego.

Please do not redline products. Guidelines for the assessment process can be found on the Intranet. All comments must be made using the coordination checklist.

<http://di.fbinet.fbi/checklist.htm>

The SAPU POC for this product is [redacted]

b6
b7C

The deadline for comments is c.o.b. 04/22/05 at 3pm.

Thank you.

[redacted]

b6
b7C

[redacted]

Program Analyst

Directorate of Intelligence
Strategic Analysis & Production Unit
Room #5431

b6
b7C

Ph# [redacted]

-----Original Message-----

From: [redacted] (SD) (FBI)

b6
b7C

Sent: Monday, April 18, 2005 4:06 PM

To: HQ_Div19 Field-Coordination

Cc: [redacted] (SD) (FBI)

Subject: Intel Assessment for review

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Attached is an intelligence assessment titled: [redacted]

b2
b7E

[redacted] for review by FBIHQ.

Please return any edits or recommended changes to IA [redacted] and SSA [redacted]
If you have any questions or concerns you may contact IA [redacted] at the below listed number.

b6
b7C

Thanks,

[redacted]

Intelligence Analyst
San Diego Field Intelligence Group (SQUAD-13)

b6
b7C

[redacted]
(fax) 858-499-7524

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED