U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

IN SHORT
TOWARD CRIMINAL JUSTICE SOLUTIONS

NIJ

www.ojp.usdoj.gov/nij | FEB. 06

NCJ 212976

Telephony Implications of Voice over Internet Protocol

Key Points

- Voice over Internet Protocol technology allows voice communications to be transported digitally through a network using Internet Protocol (IP) standards.
- Commercial IP-based telephony services are quickly proliferating as an alternative to traditional wire-line consumer telephony services.
- Traditional techniques for emergency location services at public safety answering points as well as methods for telephone intercepts and electronic surveillance (wiretaps) are ineffective or are not functional with IP-based telephony.

Voice over Internet Protocol (VoIP) communications refers to all types of conversational voice information including landline voice (telephony) or voice from a land mobile radio system. VoIP-based telephony is one of the fastest growing telecom technology sectors. Two VoIP categories are particularly relevant to public safety: VoIP telephony on public telephone networks and VoIP technology within public safety radio systems.

VoIP Market Trend

Many businesses and commercial telephony service providers are migrating to IP-based infrastructure, taking advantage of cost savings and efficiencies inherent in an IP transport network. In addition, nontraditional service providers are emerging to compete with incumbent providers by selling service that uses the Internet, cable television network infrastructure, or other nonincumbent IP infrastructure to provide access to core transport network facilities. In fact, many IP telephony services never touch the traditional telephone network.

Many free, or nearly free, personal computer/PDA-based VoIP telephony applications are readily available for download and use via the Internet. Application developers take advantage of abundant online network capacity to facilitate free Internet-only voice calls with optional access to the public-switched telephone network for a modest fee. Devices with VoIP software can communicate nomadically, functioning at any location where network access is available.

Public Safety Concerns

Identifying 911 Emergency Calls. Potential public safety concerns related to VoIP-based telephony technology include its inability to provide traditional location identification (Enhanced 911, or E911) services for 911 emergency calls placed to a public safety answering point (PSAP). IP-based telephony equipment is not tied to a specific location like wire-line based plain old telephony service (POTS). An IP-based telephone can be transported from location to location, and therefore traditional caller location

services are not available to the emergency call taker, creating PSAP procedural issues.

Meeting FCC Requirements. Recent rulings by the Federal Communications Commission (FCC)[1] mandate that commercial VoIP service providers must provide E911 services correct PSAP, but the development, implementation, and processes associated with these technologies are very immature. Incorrectly configured consumer IP devices, or devices that are moved after a location has been pinpointed, can provide false location information to an emergency call taker. A portable IP-based telephony device operating through one or more public wireless WiFi access points will not even provide the limited details that are conveyed via a typical cellular telephone device.

Conducting Surveillance. The FCC ruling also requires that a notice be attached to commercial VoIP devices that do not connect to a 911 operator. An area of lesser concern is taxation and E911 assessment fees. As service users drop traditional services and migrate to unregulated VoIP networks, disposition of E911 fees and taxes associated with the traditional telephone service is not well defined, and rules differ from State to State.

Another public safety concern is that traditional voice intercept and electronic surveillance techniques are disrupted. New techniques, tools, and infrastructure access methods are required to facilitate surveillance of IP-based telephony services. The nature of IP-based network transport makes the paths of IP packets through the network unpredictable and more difficult to intercept. Very often IP addresses associated with a specific IP-based telephony device will change regularly, making it difficult or nearly impossible to target a single device or user. Strong end-to-end encryption between IP devices can also be implemented at minimal cost, further compounding the surveillance efforts of law enforcement agencies.

Conclusion

Public safety officials and emergency call takers must be aware of these issues, and until pending regulations are fully implemented and the associated technology is available, officials must address them through education and the use of best practices. The National Emergency Number Association[2] and the Association of Public-Safety Communications Officials[3] are spearheading an effort to identify and address regulatory issues associated with VoIP telephony technology and emergency location services with the FCC. In addition, the Federal Bureau of Investigation, through its CALEA[4] Implementation Unit, has established a law enforcement executive forum to address intercept and surveillance issues associated with VoIP telephony.

For More Information

- NIJ CommTech Web site: http://www.ojp.usdoj.gov/nij/topics/commtech/.
- Regional National Law Enforcement and Corrections Technology Centers:

  Northeast (Rome, NY) 888–338–0584

  Southeast (Charleston, SC) 800–292–4385

  Rocky Mountain (Denver, CO) 800–416–8086

  Western (El Segundo, CA) 888–548–1618

  Northwest (Anchorage, AK) 866–569–2969

  Rural Law Enforcement Technology Center 866–787–2553

Notes

1. FCC Order 05–116 can be found at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-116A1.pdf.

2. Additional information can be found at http://www.nena.org/About_Contact/index.htm.

3. Additional information can be found at http://www.apcointl.org.

4. Communications Assistance for Law Enforcement Act: Additional information can be found at http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm.

NCJ 212976