

# The New Global Village



Challenges and Considerations of Lawful Intercept in an IP Environment

PTC '07

Honolulu, HI

January 15, 2007



# CALEA



- The Communications Assistance for Law Enforcement Act (“CALEA”) was passed in 1994 to define the statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization.
- All common carrier telecommunications operators must configure their networks to be “CALEA-compliant” as defined by the industry-developed J-standard. The standard defines services and features required by wireline, cellular, and broadband PCS carriers to support lawfully-authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information to a law enforcement agency.
- Law enforcement is supposed to reimburse carriers for their expense in making their networks CALEA-compliant and executing surveillance requests, but there are continuing disputes over what constitutes appropriate costs.
- In 2004, 1,710 wiretaps were executed in the United States. The overwhelming majority of wiretap requests are executed by local telephone companies because they are implemented at the first point of switching from the customer premise.

# Expanding CALEA



- The U.S. Department of Justice petitioned the FCC to apply CALEA requirements to VoIP and broadband service providers.
  
- In September 2005, the FCC applied CALEA to “interconnected VoIP” services which includes any service that can place calls to or receive calls from the public switched telephone network (“PSTN”) as well as all facilities-based providers of broadband Internet access services. This effectively encompasses:
  - VoIP services such as Vonage and Sun Rocket
  - Skype-in and Skype-out
  - Cable modems
  - DSL

# Challenges of Intercepting IP Communications



- VoIP applications are separate from the underlying transmission infrastructure
  - Identifying the appropriate party to conduct the electronic surveillance can add confusion to the process.
  - The VoIP service provider could be located overseas.
  - The target could be self-provisioning its voice services with equipment unknown to the transport provider.
  - Transport providers don't always know what type of services are on their transport.
  
- Surveillance may become overly broad
  - Transport providers may have to surveil the target's entire data flow in a converged environment.
  - Deep packet inspection may be necessary to identify voice packets.
  - The transport provider may not have the capability to identify voice packets and may have to hand off the target's entire data stream to law enforcement.

# Challenges of Intercepting IP Communications



## → Encryption

- Skype's VoIP services are encrypted.
- The target could encrypt its own communications.

## → Detection

- Targets have increasing ability to detect changes in their service performance and may be able to detect surveillance activity by their service provider.

## → Escalating Costs

- All of these challenges raise the cost of conducting electronic surveillance.
- There exists tremendous tension already between carriers and law enforcement over cost reimbursement.

## Other Considerations



- Voice is going to become a ubiquitous application
  - To what extent is society going to permit surveillance?
  - To what extent is society going to allow the Department of Justice to influence product design?
  
- What about other media?
  - What distinguishes VoIP from IM?
  - Will X-Boxes have to be CALEA compliant?
  
- What does CALEA compliance do to innovation and new product launches?
  
- How do you contend with services hosted outside of your jurisdiction?

# The New Global Village



Thank You