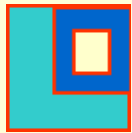


Electronic Surveillance Obligations Post 9-11

Internet Surveillance and Infrastructure
Protection Conference – May 29, 2003



Lampert and O'Connor, P.C.

Linda Kent

Mark O'Connor

1750 K Street NW, Suite 600

Washington, DC 20009

Tel (202) 887-6230

Fax (202) 887-6230

info@l-olaw.com

www.l-olaw.com

Introduction

- Since September 11, increase in law enforcement efforts to investigate, conduct surveillance
- For **communications companies**, these developments mean (1) an increase in law enforcement's efforts to monitor customer communications and (2) understanding of new laws and obligations.

The information contained in this slide presentation should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only and should not be relied upon as a substitute for obtaining legal advice applicable to your situation.

A Brief History: Development of Electronic Surveillance Laws

- 1968 - *Omnibus Crime Control and Safe Streets Act*
- 1970 - *Omnibus Crime Act*
- 1978 - *Foreign Intelligence Surveillance Act (“FISA”)*
- 1986 - *Electronic Communications Privacy Act (“ECPA”)*
- **1994 - *Communications Assistance for Law Enforcement Act (“CALEA”)***
- **2001 - *USA Patriot Act***
- **2002 - *Homeland Security Act***

Hot Topics

- CALEA Issues
 - IP Telephony
 - Broadband
 - Pending Items: FBI and FCC
- Department of Homeland Security
- FCC Activity on Homeland Security
- Pending Legislation

CALEA Compliance: A High Stakes Endeavor

- Although CALEA was enacted in 1994, certain implementation issues are still problematic for telecommunications carriers.
 - Highly technical and costly nature of requirements
 - FCC and FBI sharing responsibility for administration can make implementation confusing and difficult.
 - Lessons learned

Confusion of *CALEA* Requirements: A Serious Risk

- Law enforcement can bring an enforcement action against carriers that are not in compliance.
- Courts may impose fines of up to \$10,000.00 per day for noncompliance.
- Cost recovery has never been assured and carriers have expended substantial sums to comply with the law or sought waivers to avoid costs.

CALEA Compliance Obligations: Capability Requirements

- Applies to all wireline, cellular, and PCS providers
- Providers must ensure that their equipment, facilities and services are technically capable of isolating, enabling government interception, and delivering to law enforcement all wire and electronic communications and reasonably available call identifying information.
- Does not apply to information service providers or private networks providers.
- Carriers and manufacturers that meet an industry-formulated “safe harbor” standard are deemed to be *CALEA* compliant.
- All carriers were required to comply with the industry standard J-STD-025 requirements by **June 30, 2000** and the six additional punch list capabilities recommended by the FBI and adopted by the FCC by **June 30, 2002**.

Unresolved Applicability of *CALEA* Requirements to New Services

- FCC has required that packet-mode communications be delivered to law enforcement pursuant to J-STD-025, despite the fact that with certain packet-based technologies, such as IP communications, carriers are unable to separate call content from call identifying information.
- FCC has yet to decide whether providers of IP telephony must meet *CALEA* requirements.
- Currently, DSL services are subject to *CALEA*. The FCC's wireline broadband proceeding is currently considering modifying the classification of DSL services; FCC may not have authority to require *CALEA* compliance for DSL if the service is reclassified as an "information service."

CALEA Compliance Obligations: Capacity Requirements

- *CALEA* requires carriers to have the capacity to accommodate and “actual” and a “maximum” number of intercepts within a 24-hour period
- The statute requires the FBI to establish capacity requirements; the FCC has no authority regarding these issues.
- In January 2002, a federal appeals court vacated the FBI’s five-day requirement and remanded to the FBI the definitions of “actual capacity” and “simultaneously.”
- The FBI has not yet responded to the court’s decision.

CALEA Compliance Obligations:

Reimbursement of Implementation Costs

- Although *CALEA* provides for carrier reimbursement, the government has not allocated money to reimburse all *CALEA* expenses.
- The Statute permits reimbursement of the implementation costs for capability requirements, deployed on or before Jan. 1, 1995 that have not undergone significant upgrade or major modification, but the FBI has not yet defined what constitutes a significant upgrade or major modification.
- However, if a carrier's services or facilities are located in an area deemed high priority for surveillance by the FBI, carrier may have opportunity to obtain reimbursement of some compliance costs through fixed price agreements.

CALEA Compliance Obligations: Compliance Waivers

- The Statute permits the FCC to waive the implementation deadlines established for compliance with the capability requirements.
- Due to the difficulty of meeting these original requirements, the FBI developed the *Flexible Deployment Plan* to facilitate its review of carrier waiver requests.
- The FCC has issued instructions regarding the process for seeing such an extension.
- If *Flexible Deployment Plan* procedures were followed, carriers could expect to obtain waivers of the 2002 deadline and further waivers of the 2000 deadline until June 2004.
- Section 109(b) also permits a waiver of the capability requirements if carrier can demonstrate that compliance is not reasonably achievable. Both FCC and FBI have discouraged carriers from pursuing this remedy.

CALEA Compliance Obligations: Security Compliance Requirements

- Carriers are also required to ensure that any interception of communications or access to call identifying information is activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of the carrier.
- All carriers are required to develop and institute a policy for the supervision of employees involved in the implementation of electronic surveillance.
- This policy must be submitted to the FCC for approval; the FCC provides contact information for employee designated to assist law enforcement to FBI.

USA Patriot Act and Homeland Security Act: **Protecting National Security**

- Congress enacted both the *USA Patriot Act* and the Homeland Security Act in direct response to the September 11th, 2001 terrorist attacks.
- While *CALEA* attempts a certain pre-September 11th balance of law enforcement, privacy, and telecommunications industry interests, national security interests clearly override privacy interests in the *USA Patriot Act*.
- *USA Patriot Act* and *Homeland Security Act* affect all communications providers, including ISPs, not just telecommunications carriers.
- *USA Patriot Act* will sunset on December 31, 2005 absent further action by Congress, with only those investigations begun prior to sunset date subject to the provisions of the *USA Patriot Act* after that date.

Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers:

Expansion of Law Enforcement Authority Pursuant to *FISA*

- The most significant expansion of law enforcement authority granted by *USA Patriot Act* relates to government actions under *FISA*, which established procedures by which law enforcement monitors the agents of foreign countries.
 - While *FISA* did not permit use of information obtained under *FISA* for domestic criminal investigations, *USA Patriot Act* now permits sharing of information obtained under *FISA*.
 - *USA Patriot Act* reduces burden on law enforcement in order to obtain permission to conduct surveillance from a demonstration that “the” purpose, to “a” purpose of the surveillance is related to foreign intelligence.
 - Expands ability to obtain court orders for pen registers and trap and trace devices by including all electronic communications and extending duration of surveillance.
 - Allows for subpoenas of business records to be issued to any entity, including ISPs and other communications service providers.
 - Establishes roving wiretap authority.

**Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers:
Clarification of Authority Over Cable Companies**

- *USA Patriot Act* clarifies that ECPA governs law enforcement requests for cable subscriber records.
- Establishes that cable rules apply only when cable-viewing information is sought.

Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers:

Scope of Subpoenas for Records of Electronic Communications

- USA Patriot Act expands the previously difficult to obtain type of subscriber records that law enforcement agencies can obtain from service providers.
- Subscriber record information now includes:
 - “the means or sources of payment for...services”
 - “records of session times and duration”
 - “temporarily assigned network address(es)”

Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers:

Voluntary Disclosure of Customer Communications or Records

- While a provider of remote computing service or electronic communications service to the public cannot knowingly divulge information pertaining to a subscriber to any government entity, *USA Patriot Act* provides for an exception if the providers believes that any emergency involving immediate danger of death or serious physical injuries requires disclosure.
- *Homeland Security Act* provides an exception for communications content disclosure to a government entity where the provider believes in good faith that any emergency involving immediate danger of death or serious physical injury requires disclosure.

Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers:

Expansion of Authority to Use Pen Registers and Trap and Trace Devices

- *USA Patriot Act* expands definitions of pen register and trap and trace to include electronic communications and permits trap and trace and pen registers to capture email and stored voice mail.
- *Homeland Security Act* provides additional emergency pen register and trap and trace authority in cases where there is an immediate threat to national security or an ongoing threat to certain protected computers.

Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers:

Interception of Computer Trespasser Communications

- *USA Patriot Act* includes new authority relating to the interception of the wire or electronic communications of a computer trespasser.

Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers: Nationwide Authority

- *USA Patriot Act* allows search warrants for terrorism to be executed by a judge in any district in which activities related to terrorism may have occurred for property or persons either inside or outside the judge's district.
- Expands jurisdictional authority of a court to authorize installation of surveillance devices anywhere in the U.S.
- This will make it extremely difficult for service providers to object to legal or procedural defects in the request.

Key Provisions of the *USA Patriot Act* and *Homeland Security Act* for Communications Providers: Assisting Law Enforcement

- *USA Patriot Act* does not impose any additional technical obligations on a provider of wire or electronic communications service.
- However, if technical assistance is furnished pursuant to the *Act*, providers will be compensated.
 - There is no explanation of how compensation will be provided.

Department of Homeland Security: Defending Cyberspace

- Department of Homeland Security NPRM (April 15, 2003) to establish procedures to protect information that private sector voluntarily submits to government. Comments due **June 16, 2003**.
- Department of Homeland Security aims to identify and assess, map, issue warnings, and take preventative and protective action against current and future threats
- Bush Administration's February 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*

FCC Activities

- NRIC voluntary “best practices”
- Homeland Security Policy Council

Legislation and Electronic Surveillance

- Ongoing debate: Security interests v. privacy issues