Neustar Webinar

Effective Strategies for Ensuring Legal Compliance

September 12, 2013
Walking a Legal Tightrope
Balancing the Dual Obligations to Comply with Lawful Data Requests and User Privacy Rights

MOKERATOR:
Trevor Gray,
Supervisor, Legal Compliance Services
Neustar, Inc.

PANELISTS:
James B. Baldinger
Shareholder
Carlton Fields, PA

Pedro Pavon, CIPP/US
Associate
Carlton Fields, PA
Presentation Roadmap

- Introduction
- Demands on Carriers
- Overview of Legal Parameters
- Laws Regulating Compliance and Disclosure
- Privacy Rules in Detail
- General Responsibilities of Carriers
- Recent Developments
- Practical Recommendations
- Summary and Questions
Demands on Carriers: Overview

Service Provider

FCC & State Regulators
Shareholders
Congress & State Legislatures
Plaintiffs’ Lawyers
911 PSAPs
Civil Litigants
Privacy & Consumer Advocates
State/Local Law Enforcement
Customers
Federal Law Enforcement
New Technologies
Overview of Legal Parameters

• Legal Framework:
  » Fourth Amendment to the Constitution
  » Federal statutes, case law, and regulations
  » State statutes, case law, and regulations

• Procedural Component:
  » LEAs and civil litigants must adhere to proper procedures
  » Level of scrutiny depends on type of information sought
  » Carriers should only comply with written legal process or valid exigent circumstances requests

• Complicating Factor:
  » Old laws regulate new technologies
U.S. Constitution - Fourth Amendment

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
Federal Statutes

- **Electronic Communications Privacy Act** 18 USC §§ 2701-2711
  » Subpoena sufficient to obtain non-content information

- **Pen Register Trap and Trace Statute** 18 USC §§ 3121-3127
  » Court order required to obtain real-time incoming and outgoing digits
  » Outdated terminology – essentially “Caller ID”

- **Wiretap Statute (a.k.a. “Title III”)** 18 USC §§ 2510-2522
  » Order on “probable cause” required to access content
Federal Statutes and Regulations

• **Communications Assistance to Law Enforcement Act** – (a.k.a. “CALEA”) 47 USC § 1001-1010
  - Rules for how carriers transmit information to law enforcement
  - Requires large investment to comply
  - FCC’s CALEA Regulations 47 CFR §§ 1.20000-1.20008

• **Customer Proprietary Network Information** 47 USC § 222
  - Requires carriers to keep customer data confidential
  - FCC’s CPNI Rules 47 CFR §§ 64.2000 – 64.2011
  - FCC rules implementing CPNI law and specifying requirements

• **Cable Communications Policy Act of 1984** 47 USC § 551
  - Subscriber privacy provisions essentially CPNI for cable providers, with strict limits on disclosure of PII, especially customers’ video selections
Federal Statutes and Regulations

• Foreign Intelligence Surveillance Act (“FISA”) 50 USC §§ 1801-1862
  » Established secret court to issue surveillance orders, and permits Attorney General to issue “National Security Letters” without court approval

• “USA PATRIOT Act” Pub. Law 107-56 (2001)
  » Hastily passed after the September 11 attacks
  » Law enforcement got some “wish list” fixes to longstanding problems resulting from applying old laws to new technologies
  » Provisions were to sunset in 2005 but were extended in 2006 and again in 2011 for 4 years.
Other Statutes and Case Law

• **Various State Statutes**
  » Different requirements in each state
  » May be more (but not less) restrictive than federal
  » Alter time limitations for certain orders
  » Substantial variation in some states on civil subpoenas and exigent circumstances requests

• **Federal and State Court Decisions**
  » Interpret and apply state and federal laws, not always consistently
  » Too little case law on how to apply existing statutes to newest technologies
CALEA Requirements

- Carriers must implement systems to transmit information to law enforcement
- Must designate a senior manager responsible for intercepts and available to assist law enforcement 24/7
- Must implement measures to ensure the secrecy of interceptions and to prevent unauthorized interceptions
- Must develop written policies and procedures for compliance with surveillance requests and keep records of all interceptions
- Frequent extension of CALEA requirements to new technology
- Carriers can recover some costs of compliance, but calculating costs and establishing a cost recovery policy are difficult
- Trusted Third Parties may be used for “outsourcing” compliance
Balancing Cooperation with Privacy

“The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwanted intrusion by the State.”

*Schmerber v. California*, U.S. Supreme Court (1966)
Origin of Privacy Protections

• Fourth Amendment
  » Limits on government power on “general warrants”
  » *Katz v. United States*: Reasonable expectation of privacy test (2 parts)
    - Person must have actual expectation of privacy
    - Society must recognize expectation as reasonable
    - Exceptions (No warrant required)
      • “in public”
      • “third party” (Somewhere between these two exceptions is where most warrantless requests for data reside)
Scope of Privacy Laws

• From Strictest to most permissive, federal law has different privacy rules for:
  » Telephone monitoring and tracking of oral communication
  » Privacy of electronic communication
  » Video surveillance

• Federal law is also much more restrictive on “interception” of communication vs. retrieval of stored information
Expectation of Privacy

• Law Creates Hierarchy of Private Information
  » Subscriber, transaction, or billing info (low/medium)
  » Real-time “dialed digits,” including IP addresses (medium)
  » Location-related and location-based tracking (GPS) (high)
  » Content of communications, including stored electronic communications such as unopened email, voicemail, and voice and data communications (highest)
Privacy: Intercepting Communications

• Federal law is generally very strict
  » Interception of communications is *illegal* without a “probable cause” order, or exception:
    - Customer consent
    - Ordinary course of carrier’s business
    - Fraud prevention
  » No obligation to “look behind” order, but . . .

• Serious consequences for violations
  » Criminal penalties (fines and jail time)
  » Civil lawsuits

• Many states impose stricter privacy protections
Privacy: Stored Communications

• Stored Communications Act (SCA)
  » Enacted as part of ECPA
  » Prohibits unauthorized acquisition, alteration, or blocking of electronic communications while in storage at a telecom provider’s facility
    - For interceptions, you must consult an SCA legal expert before turning over information to law enforcement because the penalties can be severe including criminal prosecution
    - SCA also states that a provider, upon the request of government, must preserve records pending the issuance of a court order or “other process.”
Pen Register / Trap and Trace Orders

• Pen/Trap order requires lower legal standard of “relevant to an ongoing investigation” for order

• USA Patriot Act expanded scope to address new technologies by including dialing, routing, addressing, or signaling information

• Limits

  » As the emergence of “big data” makes this type of information more “identifiable,” the privacy protections in the law will increase
National Security and Privacy

• FISA, USA Patriot Act and the increased use of National Security Letters

− National Security wiretaps and other searches create a fundamental constitutional question: “where does the president’s authority leave off, and legal limits on searches apply?”

− National Security requests and traditional criminal requests may require different approaches for disclosure

− Privacy professionals within your organization must be included in determining level of cooperation and compliance with law enforcement

− The debate on “how much is too much” is ongoing and there is increased public scrutiny to broad compliance by telecommunications providers
Risk of Too Much Disclosure

• Criminal penalties and fines

• Civil lawsuits
  » ACLU, Electronic Frontier Foundation, US Privacy Council

• Public relations and regulatory nightmare
  » Social Media
  » Traditional Media
  » Customer backlash
Huge Volume of Requests

• Congressmen Ed Markey’s Report (2011)
  » Major wireless carriers responded to at least 1.3 million government requests for data.
  » Figure doesn’t include “emergency requests” or information from certain carriers.
  » Many requests were “tower dumps,” meaning the actual number of people swept up in cell phone surveillance could be thirty times higher.
  » Government reported 21,498 wiretaps from 2006-2011, but one carrier says it alone received 52,029 wiretap requests during the same period.
Recent Developments

• Edward Snowden Leaked NSA Documents (2013)
  » Government collecting information on millions of calls, routinely requests call information, including time, location, & length of calls.
  » PRISM: program to collect and store large number of communications
  » Informant: allows NSA to compile and track “metadata.”
  » NSA procedures: NSA can keep information inadvertently gathered on US citizens for up to 5 years without a warrant, if deemed relevant to prevent national security threats or to aid in future investigations.

• Other Recent Revelations
  » DEA’s surveillance of Americans’ phone records larger than NSA’s
High Profile Issue Attracts Lawsuits

- **Hepting v. AT&T**, 439 F. Supp. 2d 974, 978 (N.D. Cal. 2006) – plaintiffs alleged AT&T violated the law by honoring requests for information that were not judicially authorized.

- **Jewel v. NSA**, 673 F. 3d 902 (Ct. App. 9th Cir. 2011) - Electronic Frontier Foundation sued the NSA to stop ongoing dragnet surveillance of communications.

- **ACLU v. Clapper**, ACLU sued the NSA on its own behalf alleging illegal dragnet surveillance of communications.
Huge Public Relations Risks

• NSA director, Gen. Keith Alexander: “Intelligence gathering programs have prevented 54 terrorist attacks around the world including 13 in the United States. The intelligence community halted deadly attacks aimed at the NYSE and the NYC metro system.”

• Rep. Mike Rogers (D-Michigan), Chairman of the House Intelligence Committee: “If you can just see the number of cases where we’ve actually stopped a plot, I think Americans will come to a different conclusion than all the misleading rhetoric I’ve heard over the last few weeks.”

• Deputy FBI Director, Sean Joyce: “Intelligence gathering programs thwarted a U.S. citizen from Chicago’s attempt to bomb a Dutch newspaper.”
Pending Legislation

• Senator Leahy’s Bill:
  » Heightened requirements for obtaining records by requiring the government to show relevance to an authorized investigation.
  » FISA provisions would sunset two years early in 2015, when the PATRIOT Act expires “to ensure timely re-examination of how these authorities are being utilized.”
  » Congress will be able to address FISA and the PATRIOT Act all at once, rather than in a piecemeal fashion.
  » Proposes a formal review of Section 702 of FISA and Section 215 of the PATRIOT Act.
  » Would require increased disclosure of National Security Letters

• Several other comprehensive privacy protection legislation proposals circulating on Capitol Hill
Practical Recommendations

• Policies and Procedures:
  » Develop comprehensive written materials, and update to reflect changes in the law, technology and your company. Policies alone are dangerous if not enforced.
  » Create a Privacy Program that incorporates the need to cooperate as needed with law enforcement requests and civil subpoenas
  » Provide a Privacy Notice to customers that is clear and explains exactly how the information you collect about them will be used

• Training:
  » Educate your employees about your policies and procedures for responding to subpoenas and court orders.
  » Provide regular “refreshers” to keep up with changes in law and technology.
Practical Recommendations

**Respond:**

» Prompt compliance/response with requests is critical to keeping law enforcement “happy.”

» Educate and train senior management to provide sufficient resources.

**Compliance and Audits:**

» Regularly check on your team’s adherence to law and policies

» Use results for further training and refinement of program

**Consider Outsourcing:**

» Shift risks to vendor with proven track record
Neustar Legal Compliance Services
Legal Compliance Services (LCS) Overview

• **Experience**
  » Largest FCC recognized ‘Trusted Third Party’ (TTP), in business since 2002
  » Currently supporting hundreds of Tier 1,2,3 Communications Service Providers (CSPs)
  » As TTP, Neustar has legally authorized principal-agent relationships to receive, review, and respond to legal compliance requests on behalf of our CSP clients
  » LCS solutions enable Communications Service Providers to manage compliance obligations and risk exposures cost effectively

• **Records Production Services**
  » Provide managed services designed to mitigate the costs and risks associated with responding to legal process for the production of historical business records.
  » Conduct the legal review and validation of all legal processes to ensure the lawful disclosure of subscriber records and protect the carrier’s liability. Neustar retrieves and produces targeted subscriber communications history and customer care information from the service provider’s order management and subscriber record systems.
  » Act as the Custodian of Records produced on behalf of Neustar clients, including court appearances to testify to the authenticity of records produced under lawful process.

• **Lawful Intercept Services**
  » End-to-end managed solutions to minimize capital expenditures for non-core, non-revenue generating electronic surveillance obligations imposed by Electronic Surveillance Law (ELSUR) and Communications Assistance for Law Enforcement Act (CALEA).
  » Deploy and/or support technical platforms within carriers’ networks to fulfill CALEA compliance obligations.
  » Manage the lawful intercept function on behalf of the carrier -- the review and validation of all court records, remote provisioning of lawful intercepts--and all interaction with law enforcement, including cost recovery invoicing.
LCS Strengths

• *Experienced records production team*
  
  » Expertise in:
  
  − Legal compliance management and operations
  − Legal process review, validation, and fulfillment practices
  
  » Focused on protection of subscriber privacy while maximizing process efficiency and response accuracy to requesting parties. (Civil litigants and Law Enforcement)

• *Highly qualified technical engineering teams*
  
  » Electronic Surveillance Assistance Team (ESAT) experienced with lawful intercept (LI) technologies for diverse network architectures such as:
  
  − Wireless, IP/Broadband, VoIP, TDM, Cable, Satellite, A2G, DSL, PTP, Wi-Fi, etc.
  
  » IT Engineering (Systems Integration)
  
  − Specializing in automating retrieval and processing of CSP subscriber records via Operations and Business Support Systems (OSS/BSS) to drive down CSP costs.

• *Integrated Compliance Portal (ICP):*
  
  » Neustar’s Integrated Compliance Portal (ICP). Proprietary work process automation tool to manage full lifecycle fulfillment of compliance requests
  
  » Integration with customer data sources minimizes manual administrative efforts
  
  » Maximizes compliance accuracy, minimizes response time, cost, and risk
Questions / Comments?

Contact Us

Trevor Gray, Esq.
Supervisor, Legal Compliance Services
Neustar, Inc.

James B. Baldinger
jbalddinger@carltonfields.com

Pedro Pavon, CIPP/US
ppavon@carltonfields.com