

Customer Privacy:
What it Means for Utilities
in the Electronic Age

2005 APPA Legal Seminar
November 13-16
San Antonio, Texas

Casey Lide
The Baller Herbst Law Group, P.C.
Washington, D.C.
<http://www.baller.com>

Overview

- Federal statutory overview
 - ECPA- Stored Communications Act
 - Cable Comms. Policy Act of 1984 (s.551)
 - Telecom. Act of 1996 (CPNI)
 - Wiretap Act, Pen Register Act
- State open records laws
- Social Security Numbers
- CALEA
- DMCA
- Advice for compliance

Federal Privacy Statutes

- Electronic Communications Act of 1986
 - Stored Communications Act
 - Wiretap Act
 - Pen Register Act
- Cable Communications Policy Act of 1984
- Telecommunications Act of 1996
- Federal Freedom of Information Act
- Digital Millennium Copyright Act of 1998
- Privacy Act of 1974
- Fair Credit Reporting Act of 1970 / FACTA 2003
- Gramm-Leach-Bliley Financial Mod. Act of 1999
- Children's Online Privacy Protection Act of 1998
- Child Protection and Sexual Predator Act of 1998
- Communications Assistance for Law Enforcement Act of 1994
- USA PATRIOT Act

Statutory Overview – 4 Critical Factors

1. Type of information in question:

- Basic subscriber information
- “Other” subscriber information
- Content of communications in storage
- Surveillance (non-content)
- Surveillance (content)

Statutory Overview – 4 Critical Factors

2. Nature of service provided to subscriber:

– Communications service:

- “Cable service”
- “Telecommunications service”
- “Electronic communications service”/
Internet access
- Bundled services

– Traditional utility service

Statutory Overview – Critical Factors

3. Disclosure to whom?

- Government entity
- Private entity

4. If disclosure to government...

- criminal invest. subpoena?
- court order?
- warrant?
- wiretap order?

Stored Communications Act (ECPA Title II, 18 U.S.C. s.2701 *et seq.*)

- Addresses communications in electronic storage by a provider of electronic communications service
- Focused on information about subscribers, and content of stored communication
- Not concerned with routing/address information about communication (unlike Pen Register Act)
- Not concerned with “interception” of content (unlike Wiretap Act)

Stored Communications Act (ECPA Title II, 18 U.S.C. s.2701 *et seq.*)

- General prohibition: no person may intentionally access a facility through which an electronic communication is provided, or exceed authorization and gain access to wire or electronic communication while in electronic storage
- Main Exceptions:
 - Providers of “electronic communications services” and “remote computing services”
 - Authorized users
 - Publicly accessible

Stored Communications Act (ECPA Title II, 18 U.S.C. s.2701 *et seq.*)

- Key points for service providers (“electronic communication services,” “remote computing services”):
 - Expressly *allows* providers to disclose customer records to non-governmental parties
 - Generally prohibits providers from disclosing customer records to government entities . . .

Stored Communications Act (ECPA Title II, 18 U.S.C. s.2701 *et seq.*)

- Disclosures to government:
 - “Electronic service record”
 - Subpoena (“relevant to ongoing investigation”);
2703(d) court order; or warrant
 - “Other” account information
 - 2703(d) court order or warrant
 - Email in storage for > 180 days
 - 2703(d) court order or warrant
 - Email in storage for < 180 days
 - warrant

Stored Communications Act (ECPA Title II, 18 U.S.C. s.2701 *et seq.*)

- “Electronic service record”: (18 U.S.C. 2703(c)(2))
 - Name;
 - Address;
 - local and long distance telephone connection records;
 - session times and durations;
 - length of service and type of service utilized;
 - telephone or instrument or sub number, incl. temporarily assigned network address;
 - Means and source of payment.

Immunities and Reimbursement

- Reimbursement of costs of compliance with government order under ECPA: 18 U.S.C. 2706, etc
- A good faith reliance on a wiretap order, subpoena, court order, or grand jury subpoena provides complete defense against civil or criminal liability relating to interception or disclosure of subscriber information. 18 U.S.C. 2703, 2707

Cable Communications Policy Act of 1984

47 U.S.C. s.551 – “Protection of Subscriber Privacy”

- Applies to:
 - providers of “cable service or other service” over a “cable system” (e.g., “cable operator”)
 - “any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications services”

Cable Communications Policy Act of 1984

47 U.S.C. s.551 – “Protection of Subscriber Privacy”

- Privacy statement
 - Collection practices and use made of “personally identifiable information”
 - Length of time to maintain PII
 - Subscriber opportunity to review
 - Statement must be provided to subscriber upon commencement of service, annually thereafter

Cable Communications Policy Act of 1984

47 U.S.C. s.551 – “Protection of Subscriber Privacy”

- Collection of PII
 - Prohibited from collecting PII w/o consent
 - Exception: information necessary “to render cable service or other services” or to detect unauthorized reception

Cable Communications Policy Act of 1984

47 U.S.C. s.551 – “Protection of Subscriber Privacy”

- Disclosure of PII

- Must take all necessary actions to prevent third party access to PII
- Exceptions:
 - “necessary to render, or conduct a legitimate business activity related to, a cable or other service”
 - Pursuant to a court order, if sub. notified of the order (but see 551(h) re: ECPA)
 - Names and addresses *may* be disclosed, if sub given opportunity to prohibit or limit

Telecommunications Act of 1996

47 U.S.C. s.222 – “CPNI” Privacy Requirements

- “Customer Proprietary Network Information”
- “Telecommunications carriers”
- General duty “to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers”

Telecommunications Act of 1996

47 U.S.C. s.222 – “CPNI” Privacy Requirements

- Specific Requirements:

- “Except as required by law or with approval of the customer . . .”
- “. . . shall only use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service . . .”

HYPOTHETICAL

A subpoena issued from the local district attorney's office is received via fax at UtilCo, a public power utility that provides triple-play communications services (ISP, cable, telephony).

The subpoena instructs UtilCo to promptly turn over “all account information and any other information” maintained by UtilCo that is associated with a UtilCo subscriber, identified only by a particular IP address listed on the subpoena.

The subscriber is a customer of Internet access and video services from UtilCo.

Wiretap Act (18 U.S.C. 2510-2522)

- 1986: Title I of ECPA – “Wiretap Act”
 - Extended wiretap rules to cover interception of “electronic communications”
 - Previously Title III of Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”)
- General prohibition: “No public or private person may intentionally intercept, procure, use or disclose any wire, oral or electronic communication.”

Wiretap Act

- Exceptions to general prohibition (of many)
 - At least one of the parties consented to interception
 - Service provider intercepted in normal course of rendering service or protecting customers from harm
 - Pursuant to properly issued wiretap order by law enforcement

Is Email Subject to Wiretap Act?

- Email and the Wiretap Act: Can email be “intercepted” and subject to Wiretap Act?
 - *U.S. v. Councilman* (1st Cir., August 11, 2005):
“[T]he term ‘electronic communication’ includes transient electronic storage that is intrinsic to the communication process, and hence . . . interception of an e-mail message in such storage is an offense under the Wiretap Act.”
 - *But cf: Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003).

Wiretap Act

- State wiretap laws (40+ states)
 - Generally mirror federal scheme (must satisfy 4th Amendment)
 - Some differences in consent exceptions, and qualifying offenses for wiretap orders
 - In many states, very rarely used.

Pen Register Act (18 U.S.C. 3121-3127)

- Historically, “pen register” and “trap and trace device” were used to record impulses that identify telephone numbers dialed and received
- Pen register order not subject to 4th Amendment protections – no reasonable expectation of privacy in numbers dialed into a phone (*Smith v. Maryland*, 1979)
- USA PATRIOT Act expanded definition:
 - “a device *or process* which records or decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted”

Pen Register Act

- Burden to acquire pen register order
 - “Relevant” to ongoing criminal investigation
 - No judicial discretion: judge “shall” issue order
 - Authorizes installation of “device or process” on any wire or electronic communication service in the U.S.

Pen Register Act

- Pen register order, post-PATRIOT Act:
 - Law enforcement may obtain practically any *non-content* info about an electronic communication, including email headers.
 - Whether web-surfing data is “content” is an open question.

State Open Records Laws

- Wide variety of models
- Most have presumption of openness and accessibility for “public records”
- What entities are subject
 - In some states, government entities acting in purely proprietary capacity are *not* subject
 - “State agency” / “political subdivision”
 - Receipt of govt. funds

State Open Records Law

- What material is subject:
 - “Record” generally construed broadly
 - Electronic writings
 - In some states, limited to records of deliberation
 - “Draft” work product may or may not be subject
 - In others, mere possession by a qualifying entity
 - “Public record” probably does not include material produced *by* customers of municipally owned service provider (e.g., sub email)

State Open Records Laws

- Common Exceptions
 - Proprietary function
 - Competitive info, including customer databases, business plans
 - RFP responses, pre-award
 - Critical infrastructure / CEII
 - Trade secrets
 - Security information
 - Personal privacy
 - Traditional privileges (atty-client, etc)
 - Non-citizen requests

Social Security Numbers: Privacy Act of 1974

- Backlash against Watergate, and revelation of government's practice of keeping secret dossiers on individuals
- Imposes duties on *federal agencies* relating to maintenance of PII
 - Individual right to access, review and correct
 - Prohibited from disclosing without consent
 - Duty to destroy
 - Many exceptions

Social Security Numbers: Privacy Act of 1974

- 7(b) - Social Security Numbers:

“Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.”

-- 5 U.S.C. s.552(a)(note)

- Cannot condition service on disclosure of SSN
- Individual must prove actual damages to recover

Communications Assistance for Law Enforcement Act (CALEA)

- Enacted 1994 to ensure that law enforcement can still conduct surveillance on modern communications
- Applies only to “telecommunications carriers,” and specifically exempts “information services” – BUT...
- CALEA gave FCC authority to classify providers as “telecommunications carriers” for purposes of CALEA only, if the service is a substitute for “a substantial portion” of local exchange telephony service.

CALEA

- Sept. 23, 2005 FCC CALEA Order:
 - All facilities-based broadband Internet access providers are “telecom. carriers” for CALEA purposes, to the extent they offer services on a common carrier basis.
 - Broadband is a substitute for local exchange service in that it replaces dial-up

CALEA

- [Sept. 23 FCC Order, cont.]
 - “the fact that broadband Internet access service may be classified as an information service under the Communications Act does not determine its classification for CALEA purposes”
 - Also applies to providers of “interconnective VoIP service” – any VoIP that enables contact with PSTN is a “telecommunications carrier” for purposes of CALEA.

CALEA

- Effects and obligations
 - Enable law enforcement to intercept wire and electronic comms to and from targets of surveillance, and give access to call-identifying info “reasonably available” to the carrier
 - Specific effect on broadband and VoIP providers to be addressed in future Order
 - Compliance obligations for broadband/VoIP stayed for 18 months

Digital Millennium Copyright Act of 1998

- DMCA Subpoena power: s.512(h)
 - Special subpoena power granted to copyright holders
 - Can demand that ISPs release identity of allegedly infringing subs
 - No judicial review necessary, receiving provider “shall expeditiously disclose...”
 - BUT: ISP may have obligations from other sources to not disclose (e.g., Cable Act, Telecom Act, contract)
 - AND: s. 512(h) has been held to apply only to “hosting” function of ISP, not “conduit” function

Advice for Compliance

- Identify a PoC/expert for all privacy-related matters
- Obtain APPA's Guidebook to Federal Privacy Law
- Draft, Adopt and Distribute Privacy Policy
 - Required by Cable Act s.551
 - Enforceable by FTC
 - Include statement that provider will turn over info if required to do so by law.
 - Consider statement obligating notice to subscriber

Questions?

Casey Lide, Esq.

casey@baller.com

202/833-3301