

# “Pirating Privacy”

NATOA Annual Conference

Orlando, Florida

August 25, 2006

Casey Lide  
The Baller Herbst Law Group, P.C.  
Washington, D.C.

<http://www.baller.com>

# Privacy and Municipalities - Context

- **Municipal broadband/cable/telecom**
  - subscriber data
  - public WiFi registration data
  - Web hosting services
- **E-government**
  - Municipal websites – data collection
- **Franchising / regulatory role**
  - Cable franchisee privacy policies
- **Other**
  - Municipal surveillance camera systems

# Govt. vs. Private Actors: Privacy and the U.S. Constitution

- The term “privacy” does not exist in the Constitution
- Supreme Court: right to privacy implicit in 1<sup>st</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, 5<sup>th</sup>, 9<sup>th</sup>, and 14<sup>th</sup> Amendments (*Griswold v. Connecticut*, 1965)
- Private parties not subject to constitutional restraints; Government actors generally are

## Govt. vs. Private Actors: Fourth Amendment

- Affects government, not private entities
- Acquisition of information can rise to the level of a “search” triggering constitutional protections
- Interception of content (for example) must satisfy constitutional burden - “probable cause” requirement
- Holder of information largely irrelevant, so long as “reasonable expectation of privacy”

# Overview of Key Federal Statutes

- Since 1960, privacy law has become largely statutory, enacted against backdrop of constitutional principles.
- Federal vs. States
- A “patchwork”

# Statutory Overview – Critical Factors

## 1. Type of information in question:

- Basic subscriber information
- “Other” subscriber information
- Information about citizens (not subscribers)
- Content of communications in storage
- Surveillance (non-content)
- Surveillance (content)

# Statutory Overview – Critical Factors

## 2. Nature of service provided to subscriber:

- “Electronic communications service”/  
Internet access
- “Cable service”
- Other service (e-government, public filings,  
etc.)

# 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?

# Relevant 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
- 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

# Electronic Communications Privacy Act of 1986

- 1980s: Emergence of electronic communications led Congress to reevaluate surveillance statutes
- Three titles:
  - Title I: Wiretap Act
  - Title II: Stored Communications Act
  - Title III: Pen Register Act

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

- Applies to providers of “electronic communication service” – interpreted broadly (not just ISPs)
- Addresses communications in electronic storage
- Focused on information about subscribers, and content of stored communication
- Not concerned with routing/address information about communication (Pen Register Act)
- Not concerned with “interception” of content (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
  - Legal process

# 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
  - “Electronic service record” may be disclosed pursuant to subpoena; “other” information requires court order or warrant (ECPA – 18 U.S.C. 2703(c))

# 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.

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

*(Disclosure of records to government entity, cont.)*

- Government need not provide notice to target, and can ask court to direct a service provider to not notify the subscriber
  - Provider is not automatically prohibited from notifying

# 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 requirement
  - 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

# Cable Communications Policy Act of 1984

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

- Maintenance of PII
  - Providers must destroy PII when no longer needed for the purposes for which collected
- Damages
  - Actual damages of at least \$1,000; punitive damages, attorney fees, etc

# Cable Communications Policy Act of 1984

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

- Franchises

- State and local franchising authorities may enact other privacy measures consistent with s.551

- Franchise audits and PII

- Some cable operators have refused to share address sub info with LFA, citing privacy obligations under s.551.
- What is PII? Is an address alone “PII”?
- Is it not “necessary to render, or conduct a legitimate business activity related to...”?

# Cable Communications Policy Act of 1984

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

- Relation to ECPA

- USA PATRIOT Act made s.551 subject to providers’ obligations to assist criminal investigations under the ECPA
- Video selection habits excepted
- If not under ECPA, s.551 imposes “clear and convincing evidence” standard before disclosure to government permitted; sub must have opportunity to contest

# Immunities, Safe Harbors, 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

# ISP Immunities, Safe Harbors, and Reimbursement

- Communications Decency Act of 1996 – s.230
  - ISP “Good Samaritan” provision: ISPs that voluntarily block or screen “offensive” material directed to minors are protected from civil liability.
  - 230(c): ISP is not necessarily the “publisher or speaker” of information. Relied on for protection against tort claims (defamation etc.)

# HYPOTHETICAL

A subpoena issued from the local district attorney's office is received via fax at Brand Y ISP, a municipally owned provider of triple-play communications services.

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

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

# Email

- ECPA/Stored Communication Act - government access to email stored by service provider:
  - In storage for less than 180 days: must meet 4<sup>th</sup> Amendment probable cause standards. Requires search warrant.
  - In storage for greater than 180 days: with prior notice to sub., govt can acquire using subpoena or court order
  - Can require service provider to make backup copies

# Email

- Email and the Wiretap Act: Can email be “intercepted” and subject to Wiretap Act?
  - *U.S. v. Councilman* (1<sup>st</sup> 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).

# 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

# 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

# State Open Records Laws

- State open records laws
  - Most have presumption of openness
  - Sometimes a proprietary / governmental distinction
  - Protection of proprietary info, including customer databases, etc.
  - “Public record” probably does not include material produced by customers of municipally owned service provider
    - Could include material/email produced by employee

# Communications Assistance for Law Enforcement Act (CALEA)

- Enacted 1994 to ensure that law enforcement can still conduct surveillance on modern communications
- Covered entities must file compliance reports with FCC; “call identifying information” “reasonably available” to carrier is accessible by law enforcement
- 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

- FCC CALEA 1<sup>st</sup> R&O (Sept. 2005); 2<sup>nd</sup> R&O (May 2006):
  - 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)
  - All “interconnective VoIP” providers are subject to CALEA obligations
  - Upheld by D.C. Circuit, June 2006

# CALEA

- Effects and obligations
  - Enable law enforcement to intercept wire and electronic comms to and from targets of surveillance, and filing of compliance plans / reporting with FCC due May, 2007

Casey Lide  
The Baller Herbst Law Group, P.C.  
2014 P St NW, Suite 200  
Washington, D.C. 20036

[casey@baller.com](mailto:casey@baller.com)

[www.baller.com](http://www.baller.com)

# Digital Millennium Copyright Act of 1998

- Comprehensive update of copyright law for the digital age; ratify WIPO
- Under traditional copyright law, ISPs faced indirect liability to copyright holders resulting from conduct of subscribers.
- DMCA attempted to strike a balance between rights of copyright holders and ISPs

# Digital Millennium Copyright Act of 1998

- Three main functions of ISPs:
  1. Pure conduit of data
  2. Caching information from remote sites
  3. Hosting of information produced by subscribers.

DMCA established safe harbors...

# Digital Millennium Copyright Act of 1998

- Conduit function, caching function:
  - ISPs granted immunity from monetary damages and equitable relief related to copyright infringement by conduct of system users
  - Subject to extensive conditions and exceptions

# Digital Millennium Copyright Act of 1998

- Notice and Takedown
  - “Notification of claimed infringement” from copyright holder (formal reqs. in statute)
  - Received by ISP or registered agent
  - Prompt takedown, notice to sub., counternotification procedures
  - ISP immunized from liability to subscriber

# 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)

# Roadmap for Compliance

- Digital Millennium Copyright Act
  - Verify registered agent with Copyright Office
  - Implement policy informing subs of policy of account termination for repeat infringers
  - Post copyright compliance policy on website