

# Privacy and Community Broadband

NATOA Annual Conference

September 20, 2008

Atlanta, Georgia

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

<http://www.baller.com>

Disclaimer:

Statements in this presentation  
are not to be construed as legal advice.

# Overview

- Community Broadband Applications
  - Government functions
  - Public access
- Legal Principles
- Tough Questions
- Policy Recommendations

# Conclusions:

- Government applications using broadband networks hold great potential for more effective and efficient government services and public access.
- Privacy concerns will be raised, and could potentially derail some efforts.
- Local government (not federal) is the best entity to address such privacy concerns.

# Community Broadband: Government Functions

1. Video Surveillance / CCTV
2. Location-Based Applications
3. Wireless Sensor Applications
4. E-Government
5. Hybrids, Database Compilations

# Video Surveillance / CCTV

- Cost dropping: technology, data storage, transit
- Capabilities increasing
- Municipal wireless IP networks

= Exploding U.S. Market:

– 2005: \$9.2B

– 2010: \$21B

- Virtually all major cities, many smaller ones, special purpose areas (high crime, sensitive installations, special events)

# Video Surveillance / CCTV

- Technology development:
  - Cheap digital storage
  - Video analytics
    - License plate scanning
    - Facial recognition
    - Situational awareness
  - SCADA principles
  - Distributed feed and control (police cruisers, etc.)
  - “ShotSpotter”, etc.
  - Wireless IP

# Video Surveillance / CCTV

- Privacy Matters

- ACLU: “Surveillance society”
- Mayor Bloomberg: “It’s just ridiculous people objecting to using this technology”

- Who’s watching?

- Human? Recorded? Real-time?
- Always on or triggered?
- Can public access it? Public records? At will? Subpoena / investigation?
- Public knowledge of system information? Camera locations, applications, etc

# Govt. Services: Location-Based Applications

- GPS / cell triangulation
- Vehicle / personnel tracking
- Emergency notifications
- GIS / Google Maps/Earth integration

# Govt. Services: Wireless Sensor Applications

- Pervasive wireless network + RFID = “Internet of things”
- Wide open field for innovative applications...
  - Parking systems, traffic management
    - Beyond EZPass
    - S.F. parking trial, congestion pricing zones
    - RFID license plates?
  - Device / equipment / environment monitoring

# Govt. Services: E-Government

- Governments collect and maintain lots of personal information; more finding its way online (by design or oversight)
  - Vital records, tax info, DoT, etc
  - Virginia SSN dispute
- Tension between open records, effective e-government, and privacy

## Govt. Services: Database combinations and profiling

- Privacy threat most apparent when a variety of tools and/or databases operate together to produce a detailed and responsive dossier
- Great for advertising revenue, bad for traditional notions of privacy

# Community Broadband: Public Access Services

- Government providing communication service to the public
  - Directly: municipal / utility ISP
  - Indirectly: PPP, etc.
  - Not necessarily centrally controlled...
    - Libraries
    - WiFi bleed

## Public Access: Subscriber Record Information

- User / subscriber record information
  - Voluntarily submitted
  - PII
  - ECPA: “ISPs can share subscriber record info with any entity – except the government.”
  - Law enforcement / DMCA requests, via IP address
- Add'l requirements for cable (s.551)

# Behavioral Advertising

- NebuAd, Phorm; AT&T, Comcast, Charter, Cable One, BT, etc
- ISPs sign deal to sell web surfing habits of users; delivery of targeted banner ads, using DPI
- Supposedly only using anonymous data
- Public backlash, Congressional inquiry, NebuAd retreats...
- . . . Phorm and BT plow ahead
- Questionable opt-in plan

# Public Access: Location-Based Services

- Ad-supported networks
- San Francisco: EarthLink / Google
  - Part of EarthLink's financing of proposed free municipal wireless network in S.F. relied upon Google's ability to tailor its advertisements based on a user's location in the City.
  - Serious resistance from ACLU, community activists, re: retention policies, anonymity policies

# Legal Principles and Questions

- 4<sup>th</sup> Amendment
- Wiretap Act
- Stored Communication Act / ECPA
- Federal Privacy Act & State Counterparts
- Local / State Sunshine Laws / Open Records Acts

# U.S. Constitution

- No specific “right to privacy in Constitution. Various imputed sources (1<sup>st</sup> A., 3<sup>rd</sup> A., 4<sup>th</sup> A., 5<sup>th</sup> A., 9<sup>th</sup> A.)
- *“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.”*

-- U.S. Const. Amend.IV

# Fourth Amendment

- Obligations on government, not private entities
- Acquisition of information can rise to the level of a “search” or “seizure” requiring a warrant justified by probable cause
- 4<sup>th</sup> A. only comes into play if person has “reasonable expectation of privacy” in area or content in question.

# Fourth Amendment

- *Katz v. United States* (1967)
- Phone booth: Reasonable expectation of privacy in content of communication, but not in fact of being in a public phone booth.
- No reasonable expectation of privacy with regard to conduct in public place.
- May have privacy right with regard to communication (no audio recording, w/ CCTV)

# Wiretap Act

- Wiretap Act (18 U.S.C. 2510 – 2522)(1968)
- General prohibition: “No public or private person may intentionally intercept, procure, use or disclose any wire, oral or electronic communication.”
  - Exceptions (among many):
    - consent by at least one of the parties,
    - service provider in normal course of rendering service
    - pursuant to properly issued wiretap order
  - Net neutrality / DPI tool? (Prof. Paul Ohm)

# Stored Communication Act

- Stored Communication Act (18 U.S.C. 2701- 2712)(Title II of ECPA)
- User records and content maintained by providers of “electronic communication service.”
- Terms under which stored communication and user records can be disclosed to law enforcement
- Expressly allows providers to disclose customer records to any entity, except the government
- 2703(d) (“D” order) = compelled disclosure of stored communication if “relevant and material to ongoing criminal investigation”

# Federal Privacy Act, State Counterparts

- Federal Privacy Act of 1974 imposes duties on federal agencies re: collection and maintenance of citizen information. Duty to correct, right to inspect
- Most states have a counterpart. May or may not extend to local government entities.

# Other 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
- Foreign Intelligence Surveillance Act

# Local Open Records Laws

- Open Records Laws / Sunshine Laws = accountability. In theory.
- Public providers subject to more detailed scrutiny than private providers
- Public can obtain and potentially influence decisions about applications, privacy, data access & retention, etc.
- There were no Sunshine Laws in Oceania...

# Local Open Records Laws

- Open records laws can present a privacy issue
- Most are broad, including electronic records
- Video camera feeds and recordings?
  - Calif. Public Records Act: video camera content may be accessible pursuant to public records request.
  - Phila. Parking Authority: statute protecting video images from release
- Ephemeral “records”? (database combination, etc)

# Tough Questions

- Can targeted behavioral advertising ever be acceptable – politically or legally -- for a municipal service provider?
- Anonymization: What is PII? Name and address only? Can an IP address be considered PII?
- State action: If a PPP, at what point does it become subject to 4<sup>th</sup> A. considerations? What about use of tools from Google, etc.?
- What is the real damage of applications deemed by some to be “invasive”? An intangible worry caused by Orwell and Bentham? Or fear of actual harm? Should we adapt to a surveillance society, or fight it?

# Policy Considerations

- Appoint / identify a privacy point person or committee
- Identify community broadband applications: existing and planned
- Adopt necessary policies (video surveillance, privacy policies, data retention, etc.) BEFORE complaints emerge
- Consider changes to open records laws, if necessary
- Get educated:
  - know what to do if FBI comes knocking, or know who to call
  - understand statutory obligations

# Policy Considerations

A privacy-centric guideline:

Code of Fair Information Practices (1972):

1. *Openness*: there must be no personal data record-keeping systems whose very existence is secret;
2. *Disclosure*: there must be a way for a person to find out what information about the person is in a record and how it is used;
3. *Secondary usage*: information collected for one purpose shall not be used for another purpose without the consent of the data subject;
4. *Correction*: individuals should be able to correct or amend a record of identifiable information about the person; and
5. *Security*: any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Questions, more information:

Casey Lide

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

202.277.6276