MAKING PRIVACY THE DEFAULT

Berkeley Center for Law & Technology
2011 Spring Symposium

CA Office of Privacy Protection

- Since 2001, first in nation state office with consumer privacy focus
- Education and advocacy functions, not enforcement
  - Info and assistance for individuals
  - Best practice recommendations for organizations

Privacy = Control

- Individual's control of his/her personal information
- Fair Information Practice Principles intended to enable control
  - Transparency
  - Collection Limitation
  - Purpose Specification
  - Use Limitation
  - Individual Participation
  - Data Integrity
  - Security
  - Accountability

Regulating Policies and/or Technology

- Regulation of Policy: Data Breach Notification Law
  - Policies: Transparency & Accountability
  - Result: Better security, reduced collection (anecdotal)
- Regulation of Technology: RFID
  - Policies: Security (vs. 2dary use)
  - Result: 5 years, 10 bills, 8 vetoed, 2 enacted
- Better Regulatory Strategy?

Privacy Must Be the Default

New CA Law on Toll Collection Privacy

- SB 1268 of 2010 (Streets & Highways Code § 31490 et seq.)
- Use Limitation
  - Prohibits transportation agencies from
    - Selling or providing PII obtained from participants in electronic toll collection system
    - Using on-subscribers' PII collected through the system to market to them
    - Maximum data retention period of 4½ years
  - Requires search warrant for making PII available to LEA, with exceptions
- Transparency
  - Requires agencies to establish a privacy policy and make it available
- Accountability
  - $2500 minimum damages for misusing PII

Privacy Built In Since 1995

- Collection Limitation
  - De-identification of toll-tag numbers
  - User opt-out (Mylar bag)
- Use Limitation
  - Separate database from FasTrak
  - 24-hour data retention

Real-time Bay Area travel info from Metropolitan Transportation Commission, CHP and CalTrans.

New CA Law on Smart Grid Privacy

- SB 1476 of 2010 (Public Utilities Code §§ 8380-8381)
- Use Limitation
  - Prohibits electric and gas utilities from sharing or disclosing customer's consumption data to any 3rd party
  - Prohibits utilities from selling customer's consumption data or any other PII for any purpose
- Security
  - Requires utilities to use reasonable security procedures to protect customer's consumption data
- Transparency
  - Requires contracted monitoring svc provider to disclose its 2dary commercial use

Wiring for Privacy in Ontario

Ontario smart grid case study by HydroOne, IBM, Telvent, GE and the Information & Privacy Commissioner of Ontario

- Collection Limitation
  - Less PII available to domains outside the home
  - Minimum necessary between Customer & Services
  - None retained in Grid

Proposed CA Law on Cell Phone Privacy

- SB 102 (Correa) of 2011
- Transparency
  - Would require commercial seller of cell phones w/ geotagging to disclose the capability to potential customers before sale
- Collection Limitation
  - Would prohibit seller from selling phone with geotagging activated or operational w/out purchaser's written consent

Roadmap for Privacy on the Move

- Best Practices for Privacy by Design in Mobile Communications from Ontario IPC
- Multiple players with different roles – must collaborate
  - Device Mfr: Ensure that privacy tools are built in
  - OS/Platform Developer: Integrate controls and reporting mechanisms
  - Network Providers: Educate users and secure data
  - App Developers/Data Processors: Build privacy into development cycle, minimize data collection

Privacy by Design

- Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada
- Foundational Principles of PbD
  - Proactive not Reactive
  - Privacy as the Default setting
  - Privacy Embedded into Design
  - Full Functionality: Positive-Sum, not Zero-Sum
  - End-to-End Security: Full Lifecycle Protection
  - Visibility and Transparency: Keep it Open
  - Respect for User Privacy: Keep it User-Centric

Resources

- Privacy by Design
  - www.privacybydesign.ca
- Dorothy Glancy, "Avoiding the Matrix: How to Build Privacy into Intelligent Transportation Systems"
  - www.its.umn.edu/Events/SeminarSeries/2010/fall/october21/index.html
- California Office of Privacy Protection
  - www.privacy.ca.gov
  - See Privacy Legislation page (2010 link) for bills referenced
  - joanne.mcnabb@scsa.ca.gov