Towards Privacy By Design:
Smart Grid and Other Technologies
July 28, 2011

Sheila A. Millar
Partner
Keller and Heckman LLP
1001 G Street, N.W.
Washington, DC 20001
202-434-4143
millar@khlaw.com

Tracy P. Marshall
Partner
Keller and Heckman LLP
1001 G Street, N.W.
Washington, DC 20001
202-434-4234
marshall@khlaw.com

www.khlaw.com
Washington, D.C. ● Brussels ● San Francisco ● Shanghai

Preliminary Word

- This presentation provides information about the law. Legal information is not the same as legal advice, which involves the application of law to an individual’s specific circumstances. The interpretation and application of the law to an individual’s specific circumstance depend on many factors. This presentation is not intended to provide legal advice.
- The information provided in this presentation is drawn entirely from public information. The views expressed in this presentation are the authors’ alone and not those of the authors’ clients.
Presenters

- **Sheila A. Millar** is a Partner at Keller and Heckman and counsels corporate and association clients on a range of consumer protection regulatory and public policy matters. Ms. Millar advises clients on privacy and security policies and programs, data breach responses, data transfers and cloud computing. She also counsels clients on privacy and regulatory compliance aspects of promotions, social media policies, website terms and online sales. Noted for her expertise on children’s issues, Ms. Millar has participated in Federal Trade Commission (FTC) workshops on children’s privacy and advertising literacy.

Presenters

- **Tracy P. Marshall** is a Partner at Keller and Heckman LLP. She assists for-profit and non-profit clients with a range of business and regulatory matters. In the Internet, privacy, and advertising areas, Ms. Marshall provides counsel on e-commerce transactions and online promotions, privacy and data security policies and programs, and data breach management.
Agenda

- Privacy by Design Concept
- Survey of New Technologies
  - Smart Grid
  - RFID
  - Location-Based Services
- Best Practices

Issues

- Application of Privacy by Design concept to new technologies
- Application of existing federal, state, and international laws to new technologies and new types of data being collected
What is Privacy By Design?

- Concept developed by Ontario, Canada’s Information and Privacy Commissioner and espoused by the FTC and lawmakers
- Addressing privacy and security issues inherent with new technologies at the earliest stages of development
### The Ontario Model

- **Privacy by ReDesign: Building a Better Legacy**
  - Ontario’s Information and Privacy Commissioner
- **Roadmap for Privacy by Design in Mobile Communications**
  - Ontario’s Information and Privacy Commissioner and Arizona State University
- Incorporate privacy as a default
  - Limit data collection
  - Reduce storage time
  - Encrypt data
- **7 principles of privacy by design**
  - Proactive, not reactive; preventative, not remedial
  - Privacy as default setting
  - Privacy embedded directly 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

### FTC Privacy Report

- Provide reasonable security for consumer data
- Collect only the data needed for a specific business purpose
- Retain data only as long as necessary to fulfill the purpose
- Safely dispose of data no longer being used
- Implement reasonable procedures to promote data accuracy
- Implement privacy practices throughout the organization
- Use privacy-enhancing technologies, such as identity management, data tagging tools, and Secure Sockets Layer/other encryption technologies
Fair Information Practice Principles

- 5 core principles of privacy protection that have been adopted in the U.S., Canada, and Europe
  - Notice/Awareness
  - Choice/Consent
  - Access/Participation
  - Integrity/Security
  - Enforcement/Redress
- 7 principles under U.S.-EU Safe Harbor
- 10 principles under Canada’s PIPEDA

Department of Commerce Green Paper

- Enhancing consumer trust by adopting a comprehensive set of FIPPs to protect the privacy of personal information in commercial contexts not covered by existing sector-specific privacy laws
- FIPPs-based framework would increase clarity and promote informed consent, while fostering compatibility across industry sectors
- Recommendations:
  - Enhance transparency through privacy impact assessments that require organizations to identify and evaluate risks from the use of personal information in new technology or information practices
  - Align consumer expectations with information practices by articulating purposes for data collection and limit data use to fulfill those purposes
  - Use robust auditing systems to bolster accountability and ensure the effectiveness of commercial data privacy protections
NIST Privacy Control Catalog

- On July 19, 2011 NIST announced initial draft of Special Publication 800-53, Appendix J, Privacy Control Catalog.
  - Privacy Controls – ensures compliance with the Privacy Act of 1974 and provides guidance on:
    - Transparency
    - Individual Participation and Redress
    - Authority to Collect
    - Data Minimization and Retention
    - Use Limitation
    - Data Quality and Integrity
    - Security
    - Accountability, Audit, and Risk Management
  - Privacy controls are intended to apply regardless of an organization’s definition of PII
  - Comments due by September 2, 2011

SMART GRID
What is the Smart Grid?

- Modernization of power grid by combining two-way flow of electricity with two-way flow of information
- Two-way communications allow for dynamic monitoring of electricity use and automated electricity use scheduling
- U.S. and other countries have allocated billions of dollars to development of smart grid technology
- Responsible agencies
  - Department of Energy (DOE) has primary responsibility
  - Federal Energy Regulatory Commission (FERC)
  - National Institute of Standards and Technology (NIST)
  - Department of Homeland Security (DHS)
  - Federal Communications Commission (FCC)
  - State Public Utility Commissions (PUCs)

Benefits

- Increased energy efficiency
- Improved reliability
- Increased physical, operational, and cyber security
- Ease of repair (including remote repair)
- Consumer access to energy use information
Privacy and Security Concerns

- Identity theft and fraud
- Reveals behavior patterns
- Reveals appliances used
- Surveillance
- Home invasions

Issues

- Extent to which existing laws apply
- Who owns or can access energy usage data -- utilities, product manufacturers, consumers, third parties (governments, marketers, etc.)
- Data minimization
- Data retention, destruction
- Transparency
- Informed consent
NIST Initiatives

- **Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.** (January 2010)

- **Guidelines for Smart Grid Cyber Security** (Sept. 2010)

- **A Policy Framework for the 21st Century Grid: Enabling our Secure Energy Future.** (June 2011)
  - Focus on cost-effective smart grid investments, potential for innovation, empowering consumers, and securing the grid
  - Ensure that consumers have timely access to and control over information about energy consumption
  - Ensure protection of energy usage data consistent with FIPPs
  - Update and enhance consumer protections to address concerns about data sharing, new rate structures, and involuntary remote disconnection

Other Government Initiatives

- **FCC National Broadband Plan** (March 2010)
  - Recommendations for state action on digital energy information
  - DOE should consider consumer data accessibility when evaluating smart grid grant applications, report on states' progress on enacting data accessibility policies, and develop best practices

- **DOE Request for Information** (May 2010)
  - State efforts to enact smart grid privacy and data collection practices
  - Utility practices and policies for data access and collection, third party access to energy information, and role of consumer in balancing access and privacy

- **DOE Report on Data Access and Privacy Issues Related to Smart Grid Technologies** (October 2010)
  - Consumers should have access to and control over their detailed energy usage data, including how data is shared with third parties

- **FERC-NARUC Collaborative on Smart Response**
  - Forum for federal and state regulators to discuss smart grid policies and share best practices and technologies to harmonize policies
U.S. Smart Grid Privacy Legislation

- Electric Consumer Right to Know (e-KNOW) Act (S. 1029)
  - Introduced May 19, 2011
  - Consumers must have access to free, timely, and secure data about energy usage
  - Requires FERC to establish national standards for consumer access to energy usage data

State Legislation

- Colorado
  - Senate Bill 10-180
  - Created Colorado Smart Grid Task Force to make recommendations on the feasibility, cost, and timing of transitioning to a secure smart grid
  - Task Force released report in January 2011 on Deploying Smart Grid in Colorado: Recommendations and Options

- Oklahoma
  - Electric Utility Data Protection Act (H.B. No. 1079)
  - Approved by Governor on May 20, 2011
  - Utilities must provide customers with reasonable access to information, provide copy of access to usage data upon request, and maintain confidentiality
  - Utilities may use customer-identifiable usage data for internal business purposes and share with third party service providers without consent
California PUC Proposed Rules

- May 6, 2011: PUC issued proposed decision addressing smart grid privacy and security; sought comments; rules pending
- Incorporate FIPPs
- Apply to customers of investor-owned electric utilities offering or proposing to install smart meters and companies the utilities contract with
- Require notice and privacy policy for the collection, storage, use and disclosure of usage information obtained through smart meters when associated with information that can reasonably identify a customer
- Customers could access and control use and disclosure
- Would not cover usage information from which identifying information has been removed so that a customer cannot be identified or re-identified
- Utilities could collect, store, and use information without consent to provide services; other entities generally must have prior consent
- Entities must implement administrative, technical and physical safeguards to protect information and notify PUC of a breach affecting 1,000 or more customers

International Smart Grid Initiatives

- **EU**
  - EC Communication on *Smart Grids: from innovation to deployment* (April 2011)
    - Focuses on developing technical standards (the Privacy by Design approach), ensuring data protection for consumers, establishing a regulatory framework to provide incentives for smart grid deployment, guaranteeing an open and competitive retail market, and providing support to innovation for technology and systems
    - Clarifies the legal framework applicable to smart metering

- **Canada**
  - Report on *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study* (April 2011)
    - Guidance document for utilities to embed privacy into smart grid
What Is RFID?

- Radio Frequency Identification
- Location and data tracking tool
- Simple RFID tag consists of a microchip and antenna that sends back information via radio waves when brought near a remote “reader”
- RFID has raised privacy concerns due to the linking of personal information with RFID tags
Benefits of RFID

- Automatic inventory management system
- Very small (as compared to UPC codes)
- Can be used to quickly and easily track consumer preferences

Privacy and Security Concerns

- “Skimming”
  - RFID readers can surreptitiously pull data from tags without a holder’s knowledge
- Surveillance
  - RFID tags can be planted inconspicuously to track people and items
- Purchase/ location tracking
  - Merchandise purchases tied to personal information
U.S. RFID Legislation

- Approximately 14 states have RFID privacy laws
- Many of the laws relate to use of RFID in driver’s licenses or vehicles
- CA prohibits remotely reading a person's ID document using RFID without consent
- RI prohibits use of RFID to track students

EU Framework for RFID Privacy

- EU RFID Privacy and Data Protection Impact Assessment Framework (January 2011)
  - Signed by European Commission, European data protection and information security authorities, NGOs and industry groups
  - Establishes a self-regulatory mechanism for ensuring data protection in the field of RFID
  - Companies to conduct an assessment of privacy risks and take measures to address risks before a new RFID application is introduced
  - Includes detailed procedures to enable the delivery of RFID applications in compliance with the Data Protection Directive (95/46/EC) and e-Privacy Directive (2002/58/EC)
What Is Geolocation Information?

- Information generated by electronic devices (cell phones, Wi-Fi equipped laptops, GPS navigation units) that can be used to determine the location of the devices and their owners
- Emerging issue for mobile
Examples of Location-Based Services

- Navigation
- Locating the nearest ATM or restaurants
- Locating a friend or employee
- Parcel and vehicle tracking
- Delivering coupons or advertising to consumers based on their current location

The LBS Controversy

- Report in April 2011 that Apple iPhone gathered location data and stored it in an unprotected, unencrypted format – even when location-based tracking turned off
- Apple made changes to iPhone storage in response
  - Limit storage of location-based data to one week
  - Stop transferring location-based data from device to user’s computer
  - Allow users to delete all location-based data collection
  - Encrypt location-based data stored on the device
- Research prompted scrutiny into Google’s Android software, which was also tracking location data
  - Location data was sent with data containing a unique ID
Class Action Lawsuits

- Both suits allege violations of the Computer Fraud and Abuse Act and state laws
- Both suits seek injunction and monetary damages

Congressional, Regulatory Action

- **March 30, 2011**: Reps. Edward Markey (D-MA) and Joe Barton (R-TX) sent inquiries to AT&T, Verizon, Sprint, and T-Mobile about their data collection, storage and disclosure practices for PII
- **April 21, 2011**: Rep. Ed Markey (D-MA) and Sen. Al Franken (D-MN) sent letter to Apple expressing concerns about collection of location information
- **April 25, 2011**: Congressmen sent a letter to Google, Apple, Research in Motion, Nokia and HP in questioning their privacy policies for location information
- **May 10, 2011**: U.S. Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law held a hearing on *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy*
- **June 28, 2011**: FCC and FTC held a forum on the use of smartphone location data for targeted ads and other purposes
- **COPPA Review** (ongoing) also evaluating LBS implications for kids
Do Not Track Online Act of 2011 (S. 913)

- Sen. Jay Rockefeller (D-WV)
- FTC to establish opt-out mechanism for preventing collection and use of “personal information” relating to both online and mobile apps
- Enforcement: state attorneys general; FTC intervention; penalties up to $15 million

Geolocation Privacy and Surveillance Act (S. 1212)

- Sen. Ron Wyden (D-OR) and Rep. Jason Chaffetz (UT)
- Modeled after federal wiretapping statutes
- Applies to information generated by or derived from wireless devices and tracking devices
- Law enforcement must obtain a warrant to obtain geolocation information
- Limits the use of geolocation information in court unless proper procedures are followed
- Exceptions where individual is reasonably believed to be in danger or requested assistance, geolocation information is publicly available, mobile electronic device was stolen, or individual consented
- Individuals whose location data was intercepted, disclosed, or intentionally used in violation of the law can file a civil lawsuit and recover actual damages or $10,000 in statutory damages
Location Privacy Protection Act of 2011 (S. 1223)

- Sen. Al Franken (D-MN) and Sen. Richard Blumenthal (D-CT)
- Applies to service providers (e.g., Apple and Google) and app developers
- Express consent required before collecting and sharing location data from a consumer
- Any service provider that collects data from > 5,000 devices must take reasonable steps to safeguard the data and delete the data upon request
- U.S. Attorney General, State AGs, and consumers can bring civil action

Lessons Learned From Google Street View

- Privacy Commissioner of Canada investigated Google’s collection of PI from unsecured wireless networks for violations of PIPEDA

- Commissioner satisfied with Google’s response
  - Augmented privacy and security training provided to employees
  - Implemented a system for tracking projects that collect, use or store PI and for holding responsible individuals accountable for privacy
  - Required project leaders to draft, maintain, submit and update Privacy Design Documents for all projects
  - Assigned an internal audit team to conduct periodic audits to verify the completion of selected Privacy Design Documents
  - Initiated a review process whereby Privacy Engineering, Product Counsel and Privacy Counsel teams review proposals involving location-based data and programs to be used for data collection

- Google must undergo independent, third party audit of its privacy programs within a year and share the results with the Commissioner
Best Practices

- Create company awareness
  - Understand FIPPS
  - Foster culture of privacy, security
- Assign responsibilities
- Review applicable laws and guidelines
- “Know, Say, Do”
Best Practices

- Seek to understand technological capabilities
  - Implications and limits of privacy by default for functionality, customer service, marketing
- Conduct privacy impact assessments
- Establish policies and procedures
  - Address sharing data with third parties
- Implement, maintain security

Conclusion

Privacy and security: a goal and a journey

- Privacy doesn’t exist without security
- Security alone doesn’t guarantee privacy
- Lapses in privacy and security are leading to increasing pressure to adopt new legislation and restrictions
- Incorporating “privacy by design” and FIPPS can help maintain trust, minimize PR, regulatory, litigation fallout
Questions?

www.khlaw.com
Washington, D.C. ● Brussels ● San Francisco ● Shanghai

Thank you!

Sheila A. Millar
Partner
Keller and Heckman LLP
1001 G Street, N.W.
Washington, DC 20001
202-434-4143
millar@khlaw.com

Tracy P. Marshall
Partner
Keller and Heckman LLP
1001 G Street, N.W.
Washington, DC 20001
202-434-4234
marshall@khlaw.com

www.khlaw.com
Washington, D.C. ● Brussels ● San Francisco ● Shanghai