Automotive Privacy

A discussion of privacy and security legal compliance for the automotive industry

FOLEY

FOLEY & LARDNER LLP

Your Speakers

Chanley Howell, CIPP/US
Foley & Lardner LLP
One Independent Drive, Ste 1300
Jacksonville, Florida 32202
(904) 359-8745
chowell@foley.com

Adam Losey
Foley & Lardner LLP
111 North Orange Avenue
Orlando, Florida 32801
(407) 244-7136
alosey@foley.com

Rules of the Road

3

- US Sectoral v. EU Comprehensive
- Alphabet soup (FCRA, FACTA, GLBA, HIPAA, FERPA, TCPA, CAN-SPAM)
- State laws – Security breach notification, Social Security numbers, and data security (e.g., Mass., Nevada)
- FTC Consent Decrees, Commentary and Guidelines
- Court cases and precedents

FTC March 2012 Report

4

- Privacy By Design
- Simplified Choice
- Greater Transparency
  - » Privacy Notices
  - » Access
  - » Consumer education

FTC March 2012 Report

5

- Affirmative opt-in consent to collect location information
- Limit collection to data needed for the requested service or transaction
- Prominent notice for sharing of data
- Do Not Track
- Mobile

NTIA 2012 Report

6

- National Telecommunications & Information Administration (Dept. of Commerce)
- Consumer Privacy Bill of Rights
- Control over collection and use of personal information
- Clear notice and transparency regarding companies' data privacy and security policies and practices

Location-Based Services

- Disclosure
- Consent and controls
- Safeguards and retention
- Accountability

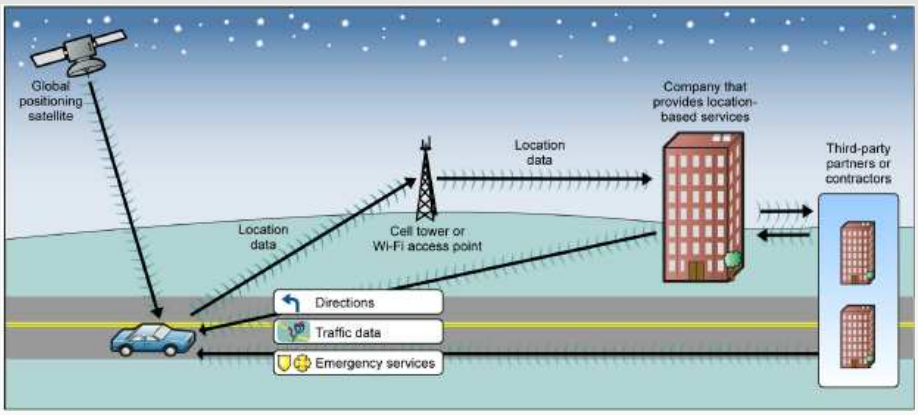
In-Car Location-Based Services

Systems or devices that deliver in-car location-based services	Description	Examples
Telematics systems 	• Provided by auto manufacturers. • Consumers receive services through devices embedded in their cars or through their mobile devices that are connected to their cars.* • Services are generally subscription-based, requiring consumers to pay for services.	General Motors' OnStar, Ford Sync, Chrysler UConnect
Portable navigation devices (PND) 	• Provided by PND companies. • Consumers receive services through PNDs that are equipped to transmit location data, or through their mobile devices that are connected to their PNDs.* • Services can be free to consumers or require a fee for subscription.	TomTom, Garmin
Map and navigation applications for mobile devices 	• Provided by mobile application developers. • Consumers receive services through smart phones. • Services are generally free or relatively inexpensive.	Scout GPS Navigation, Google maps

- GAO In-Car Location-Based Services Report, Fig 1 (Dec 2013)

9

Typical Data Flows



- GAO Report, Fig 2

10

Industry-Developed Privacy Practices

- Disclosures to consumers about data collection, use, and sharing
  - » State reasons companies collect and share data.
  - » State specifically that collection of location data is limited to specific needs.
  - » Do not use data for a purpose other than what has been disclosed to consumers without providing notice and obtaining consent before using the data.

Controls Over Location Data

11

- Obtain consumers' consent before collecting their personal information.
- Provide consumers the ability to opt out of data collection to which they have previously consented.
- Allow consumers to delete location data that have been collected. (Noted as industry deficiency in GAO Report.)

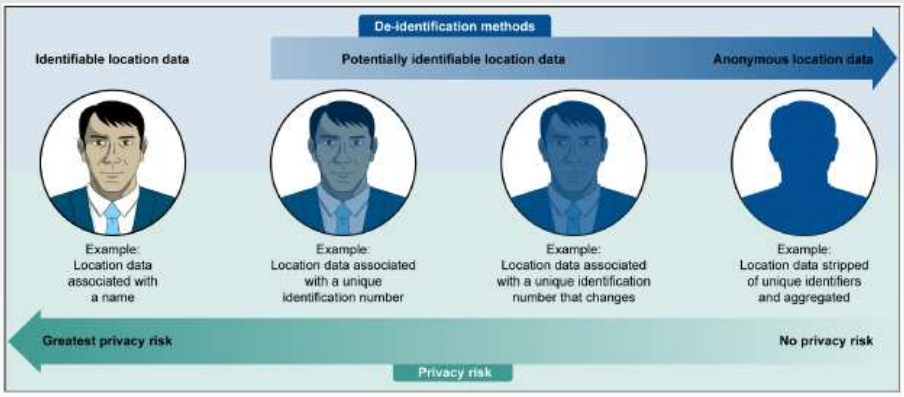
Data Safeguards and Retention

12

- State a specific time frame for retaining consumer data.
- Protect data with reasonable security safeguards against risks such as loss or unauthorized access.
- De-identification.

13

De-Identification



- GAO Report, Fig 3

14

Accountability of Third Party Service Providers

- Contractually require service providers to protect privacy and security, and/or comply with certain privacy and security practices
- Limit or prohibit commingling data with data from other customers
- Due diligence risk assessments
- Audits or risk assessments of the service provider

15

Accountability

- State a specific time frame for retaining consumer data.
- Protect data with reasonable security safeguards against risks such as loss or unauthorized access.

16

Monetizing Data/Data Brokers

- Data Broker is potentially very broad term
- Any company that collects personal information
  and distributes to a third party
- Particular concerns regarding sensitive information
  (SSN, DLN, TIN, credit and bank account information, health information)
- Transparency (notice, choice and access)

De-Identification

17

- If done properly, can remove data from some or all requirements of privacy and security laws
- HIPAA methods as a guide (Safe Harbor, Expert Determination)
- No reasonable likelihood or re-identification

Online Behavioral Advertising

- Collecting online activity across multiple websites to deliver interest-based advertising
- Self-regulatory programs
- Digital Advertising Alliance
- California OPA (CBC § 22575)

Mobile

- FTC Mobile Privacy Disclosure (2/2013)
- Privacy Policy available through app store and clearly identified in app
- Just in time disclosures and affirmative consent for collection or sharing of sensitive information (financial, health, location, children)
- Disclosures regarding sharing with ad networks and other third parties
- Consider participating in self-regulatory programs

Compliance Best Practices

- Develop a PI inventory & practices
- Identify applicable laws and standards
- Identify gaps between legal requirements and intended PI practices
- Remediate gaps and determine methods for complying with applicable laws and standards

Develop a PI Inventory

- Categories of PI and Sensitive PI collected
- How collected
- Where stored (physically and geographically)
- Purposes for collecting and intended uses
- Individuals requiring access
- Sharing with and access by third parties

Identify Applicable Laws and Standards

- FCRA
- GLBA
- HIPAA
- COPPA
- FERPA
- TCPA
- CAN-SPAM
- FTC Reports & Guidance
- PCI DSS
- Privacy Policies
- DAA OBA Guides
- MMA Text Messaging

Identify Gaps

- Intended practices v. legal requirements and standards
- Notice
- Purposes (e.g., marketing v. transactional)
- Choice
- Access
- Sharing
- Security

Close Gaps and Determine Compliance Methods

- Notice
- Choice
- Access
- Accuracy
- Transfers to third parties
- De-identification
- Limiting collection and storage
- Security
- Documentation (policies, notices, etc.)
- Education and training

Thank You

Chanley Howell, CIPP/US
Foley & Lardner LLP
One Independent Drive, Suite 1300
Jacksonville, Florida 32202
(904) 359-8745
chowell@foley.com

Adam Losey
Foley & Lardner LLP
111 North Orange Avenue
Orlando, Florida 32801
(407) 244-7136
alosey@foley.com

For more insight on automotive privacy, and other issues facing the industry, subscribe to our blog – Dashboard Insights, www.autoindustrylawblog.com