

**In-Vehicle Black Boxes:  
Current Federal  
Legislation and  
Regulation, and the  
Issues They  
Address/Create**

**Robert B. Kelly, Esq.**

**Mark D. Johnson, Esq.**

**TRANSPRO 2010**

**December 14, 2010**

**SQUIRE  
SANDERS**

LEGAL  
COUNSEL  
WORLDWIDE



# Privacy and Event Data Recorders (EDRs)

- EDRs record vehicle status and change in status before, during and after an accident, including:
  - Vehicle speed, braking, changes in velocity and direction, airbags, use of seat belts, etc.
  - Devices continually record, and then overwrite information, until a “triggering” event occurs, retaining the crash data from a few seconds before, during and after the accident
  - Do not record personally identifiable information, i.e., owner’s name
- How is privacy implicated?
  - Who owns the data?
  - Who can access the data?
  - How can the data be used?

# National Highway Traffic Safety Administration

- NHTSA has primary regulatory authority
- Current Rules – 49 CFR Part 563 (effective October 2006)
- Do not mandate installation of EDRs
- However, for light vehicles manufactured after September 1, 2012, installed EDRs must follow:
  - Standardized format for collected data
  - Prescribed recording intervals for each data element
  - Notice statement in owner's manual
- While acknowledging privacy concerns, NHTSA did not address – citing lack of statutory authority

# Federal Legislation

- Complementary bills in current Congress
  - HR 5381
  - S 3302
- Vehicle owner/lessee is the owner of EDR data
- Limited disclosure mechanisms
  - Consent of vehicle owner/lessee (including for vehicle diagnostics, repair, and service)
  - Court Order
  - By government motor vehicle safety agency (but only where VIN and owner's name stripped from data)
- Any action would need to be before end of current Congress

# State Action

- At least 13 States have passed laws addressing EDRs:
  - AR, CA, CO, CT, MA, ME, ND, NH, NV, OR, TX, VA, WA
- Sample state law provisions:
  - Presence of EDRs must be revealed to vehicle owner/lessee
  - Vehicle owner/lessee is “exclusive” owner of EDR data
  - EDR data is “personal information of vehicle owner” or “tangible” property of vehicle owner
  - Limited disclosure to third parties (owner consent, court order, government safety agency, or vehicle repair/diagnostics)
  - Law enforcement access by search warrant based upon finding of probable cause
  - Insurers cannot require owner/lessee consent as a condition of coverage or settlement of claim
  - Vehicle owner/lessee retains ownership of data after accident, including when vehicle is salvaged
  - Data made available to government safety agency without name of owner or driver and abbreviated VIN (so cannot identify specific vehicle)
  - If EDR part of a subscription service, *i.e.*, OnStar, subscription agreement must disclose what data is recorded and transmitted

# Reported Cases: Issues

- Presence of probable cause for police search warrant to access EDR data
- Determining valid owner's consent to police accessing EDR data
- Admissibility of EDR data at trial
  - Under traditional evidence rules
  - As “scientific evidence” produced by expert witness (accident reconstruction)

# Technology

- Even if vehicle owner/lessee “owns” the EDR data, there is still a technical barrier to access
- Police, insurance companies, vehicle OEMs and dealerships more likely to have technical ability to access data
- Current NHTSA Rules did not mandate a common technical means of access
- Existing proposals for common technical access tools:
  - “Mechanical lockout” system on vehicle diagnostic port designed for sole use and control of vehicle owner
  - IEEE Standard 1616a – Technical protocol to prevent tampering with (erasing, modification) of EDR data or improper downloading

# ITS and Privacy

EDRs are not the only ITS technology implicating privacy -

- Electronic tolling (financial and location information)
- Congestion pricing (financial and location information)
- Cellular and other “probe” technologies for dynamic navigation and traffic conditions (location information)

**These and other information-based ITS services and products will likely implicate privacy concerns,**

**BUT ...**

# ITS and Privacy

**... while privacy concerns cannot be eliminated – they can be managed.**

- Privacy “By Design” – Consider privacy in design and implementation of ITS systems and services – from initial conception through deployment and operation
- Limit amount and types of data to be collected only to that information actually needed to provide the product or service
- “Anonymize” data whenever feasible
- Limit what data is retained and the period of time it is stored
- Limit disclosure to third parties

**Robert B. Kelly, Esq.**  
**Mark D. Johnson, Esq.**  
**Squire, Sanders & Dempsey**  
**L.L.P.**

**Washington, DC**

**(202) 626-6216**

**[RKelly@ssd.com](mailto:RKelly@ssd.com)**

**(202) 626-6265**

**[MaJohnson@ssd.com](mailto:MaJohnson@ssd.com)**

**SQUIRE  
SANDERS**

LEGAL  
COUNSEL  
WORLDWIDE

