“We need to look at the data we can get out of cars and ask how we can leverage this intangible.”

EY Business Leaders Roundtable
Dec. 2013

“Connectivity is gradually turning the automobile into a highly efficient data harvesting device.”

Telematics Update
Oct. 6, 2014
Types of Personal Data in Car Systems

- Identification data
- Customer Account data
- Vehicle Health data
- Driver Behaviour data
- Biometric and personal health data
- Location data
- Personal communications
- Personal contacts and schedule
- Infotainment preferences and use
Privacy Risks

• Security breaches
  • opportunistic crime
  • organized crime
  • stalkers

• Statutorily permitted third party access
  • state surveillance
  • debt collection
  • law enforcement, litigation, investigation

• Unexpected and undesired secondary uses
  • targeted marketing
  • function creep
  • discrimination in service provision
Vehicle Health Report Privacy Notice

When you run a Vehicle Health Report, Ford Motor Company may collect your cell phone number (to process your report request) and diagnostic information about your vehicle. Certain updates to Vehicle Health Report may also collect additional vehicle information. Ford uses the vehicle information it collects, as well as information regarding individual access to Health Reports at www.syncmyride.com for any purpose. If you do not want to disclose your cell phone number or vehicle information, do not run the feature.

Refer to your Owner Support Account -- Privacy Statement for more information.

Because SYNC provides service through wireless networks, we can’t promise that your communications won’t be intercepted by others. You agree we won’t be liable for any communications loss of privacy occurring in communication over such networks.
COMMITMENT
OF THE
ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
AND THE
ASSOCIATION OF GLOBAL AUTOMAKERS, INC.
TO THE
CONSUMER PRIVACY PROTECTION PRINCIPLES
FOR
VEHICLE TECHNOLOGIES AND SERVICES

The members of the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers, Inc. take the privacy of customers very seriously. We believe that strong consumer data privacy protections are essential to maintaining customers’ trust.

To demonstrate this commitment to our customers, members of the two Associations came together to create the Consumer Privacy Protection Principles for Vehicle Technologies and Services (“Principles”), to which we hereby subscribe and agree to as a baseline commitment to data privacy. We encourage other members of the automotive community to join our commitment and subscribe to these Principles as well.

The Principles reflect a major step in protecting personal information collected in the vehicle. For the first time, the industry is adopting central concepts to demonstrate a unified commitment to the responsible stewardship of information used to provide vehicle technologies and services. Sensitive information, such as geolocation, driver behavior, and biometric information, receives additional, heightened protections under the Principles.

The Principles reflect the reality that automobiles increasingly rely on innovative technologies and services that are designed to enhance vehicle safety, improve vehicle performance, and
Privacy Analysis: Law

- Openness
- Accountability
- Purpose Specification + Notice
  - Appropriate Purposes
- Consent
- Limiting Collection & Retention
- Limiting Use & Disclosure
- Security Safeguards
- Accuracy
- Individual Access
- Challenging Compliance
PIPEDA analysis: Results

X Openness
  • Policies not publicly available
  • Purposes often vague and open-ended

X Accountability
  • OEMs don’t take responsibility for dealers
  • OEMs don’t take responsibility for data in transit

X Purpose Specification / Notice
  • Purposes often vague and open-ended
  • No effective method of notice; often assumed by virtue of use
PIPEDA analysis: Results

X Limits on Collection (and Retention)
  • No clear limits on data collection or retention
  • No industry standards for retention

X Limits on Use and Disclosure
  • Wide range of uses, not clearly specified
  • Unnecessary uses and disclosures without even opt-out

X Consent
  • No choice re: non-essential uses
  • Refusal to deal with customers who don’t agree to secondary uses
PIPEDA analysis: Results

X Individual Access
  • Very limited individual access to own data

X Security Safeguards
  • General assurances only
  • No industry standards
  • Some express disclaimers
The Context

- Cars are not a luxury
- Limited choice (no “pick and pay”)
- Limited time
- Other purchasing considerations
- No competition on privacy
- Multiple privacy policies requiring “agreement”
- Difficult to figure out impact on privacy

Is consent even possible in this context?
Recommendations

1. Establish data protection standards for the industry
   - consistent with (under?) PIPEDA
   - like *Motor Vehicle Safety Standards*
2. Develop *national* data protection standards for usage-based auto insurance
3. Involve privacy experts in development of public Intelligent Transportation Systems
4. Adopt “Privacy by Design” principles now!
THE CONNECTED CAR:
WHO IS IN THE DRIVER’S SEAT?

A study on privacy and onboard vehicle telematics technology

https://fipa.bc.ca/connected-car/