

Why Cars Need Free Software

Alison Chaiken, she-devel.com, March 24 2012

“no data are recorded by the EDR under normal driving conditions and no personal data . . . are recorded. However, other parties, such as law enforcement, could combine the EDR data with the type of personally identifying data routinely acquired during a crash investigation.”

Source: Insurance Institute for Highway Safety,
<http://www.iihs.org/research/qanda/edr.html>



Publishing my own source with Personal Genome Project



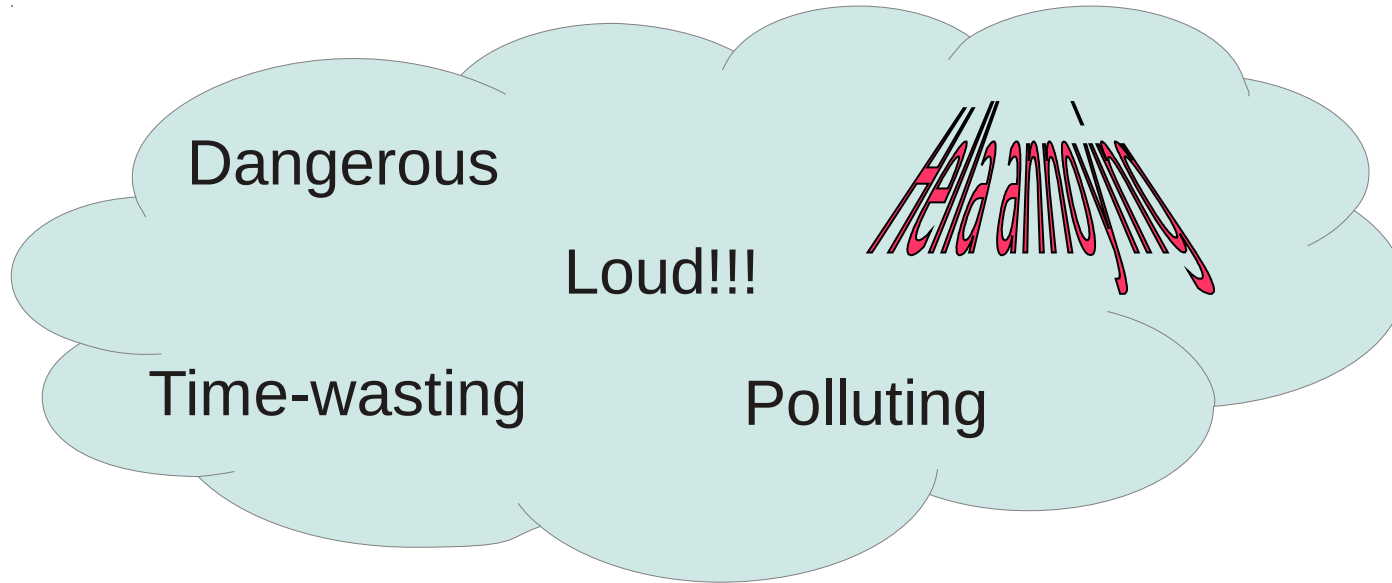
Feel free to fork and improve me!

Same Old Topics

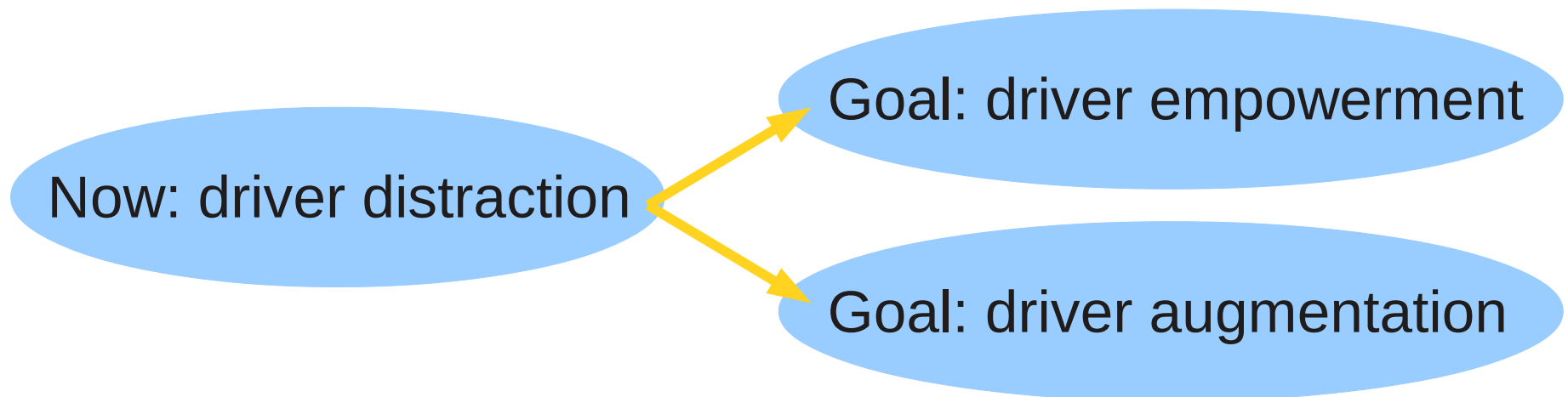
- Security
- Privacy
- Personal empowerment

reappear on a new platform.

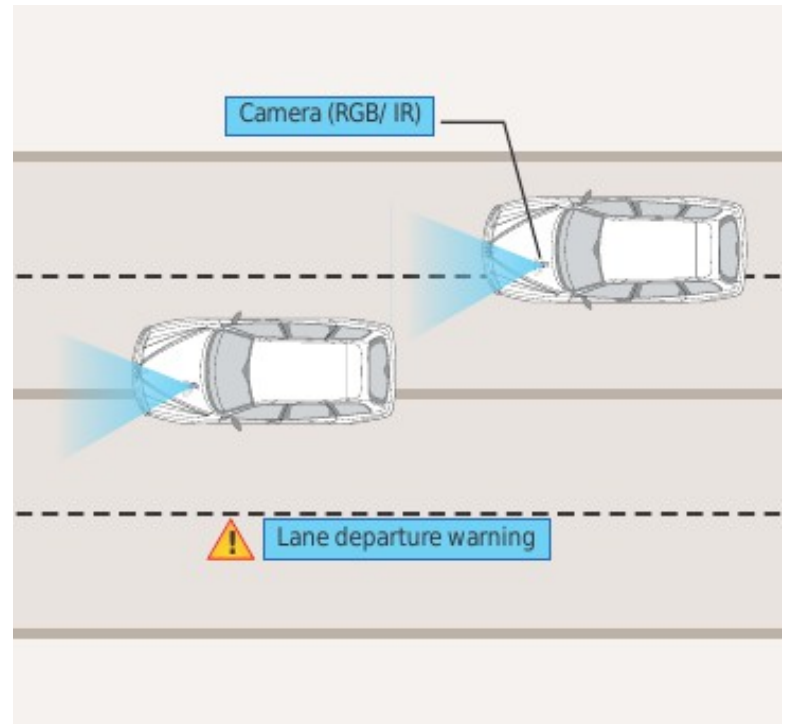
Our transportation system is



because *until now* individuals had little power to change it.



What is “in-vehicle infotainment”?



Courtesy Tata Consultancy Services

What “infotainment” calls to mind

What IVI could be

Status of Automotive Free Software

Manufacturer	Confirmed Operating system
Fiat-Chrysler Blue&Me (500, Delta), Kia Uvo, BYD	Microsoft Windows Embedded Automotive
Ford (all?)	MyTouch/Sync-Microsoft; OpenXC-Android
General Motors/Cadillac User Experience	MontaVista's GNU/Linux
Geely (China); Hawtai (China)	GNU/Linux: Moblin (MeeGo predecessor)
Renault R-Link	Android
Honda (Accord, Odyssey, Pilot), Audi, BMW (7-series and M models), Chrysler, Daewoo, GM (OnStar), Hyundai, Land Rover, Porsche, Saab (9-3) Renault (SM7)	QNX

Linux Foundation members: Toyota, Pelagicore, Symbio, Tieto

Automotive Linux Summit 2011 presenters: Toyota, Nissan, BMW

MeeGo Conference 2011 presenter: Nissan

Volkswagen has a pilot using Maemo (GNU/Linux).

Current Automotive Security Situation is Shaky



Source: <http://www.autosec.org/>

Wheels

The Nuts and Bolts of Whatever Moves You



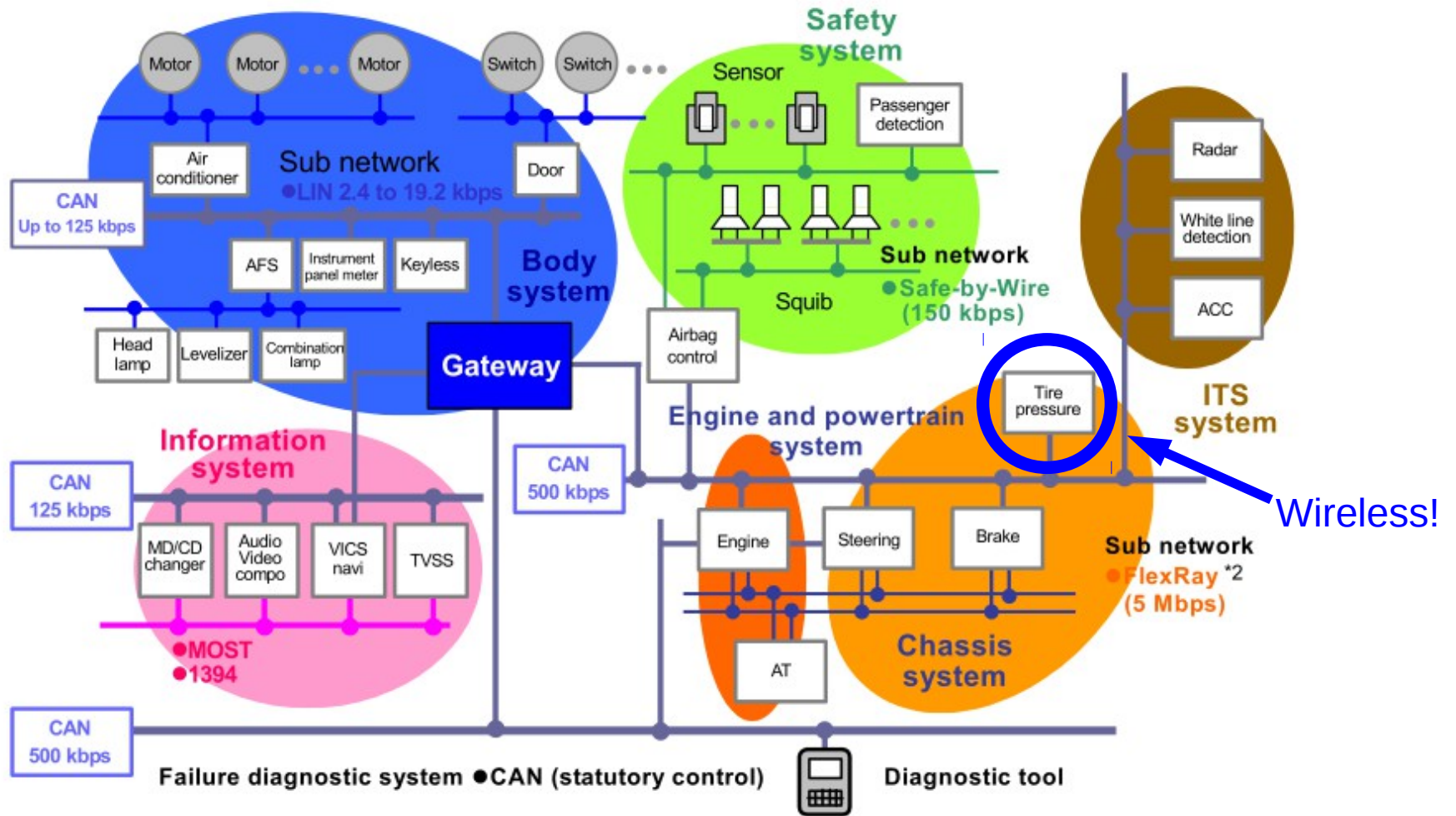
June 16, 2011, 12:49 PM

Nissan Leaf Telematics May Leak Driver Data to Third Parties

By JOHN R. QUAIN

Source: NY Times

Gateways pass information freely among subnets

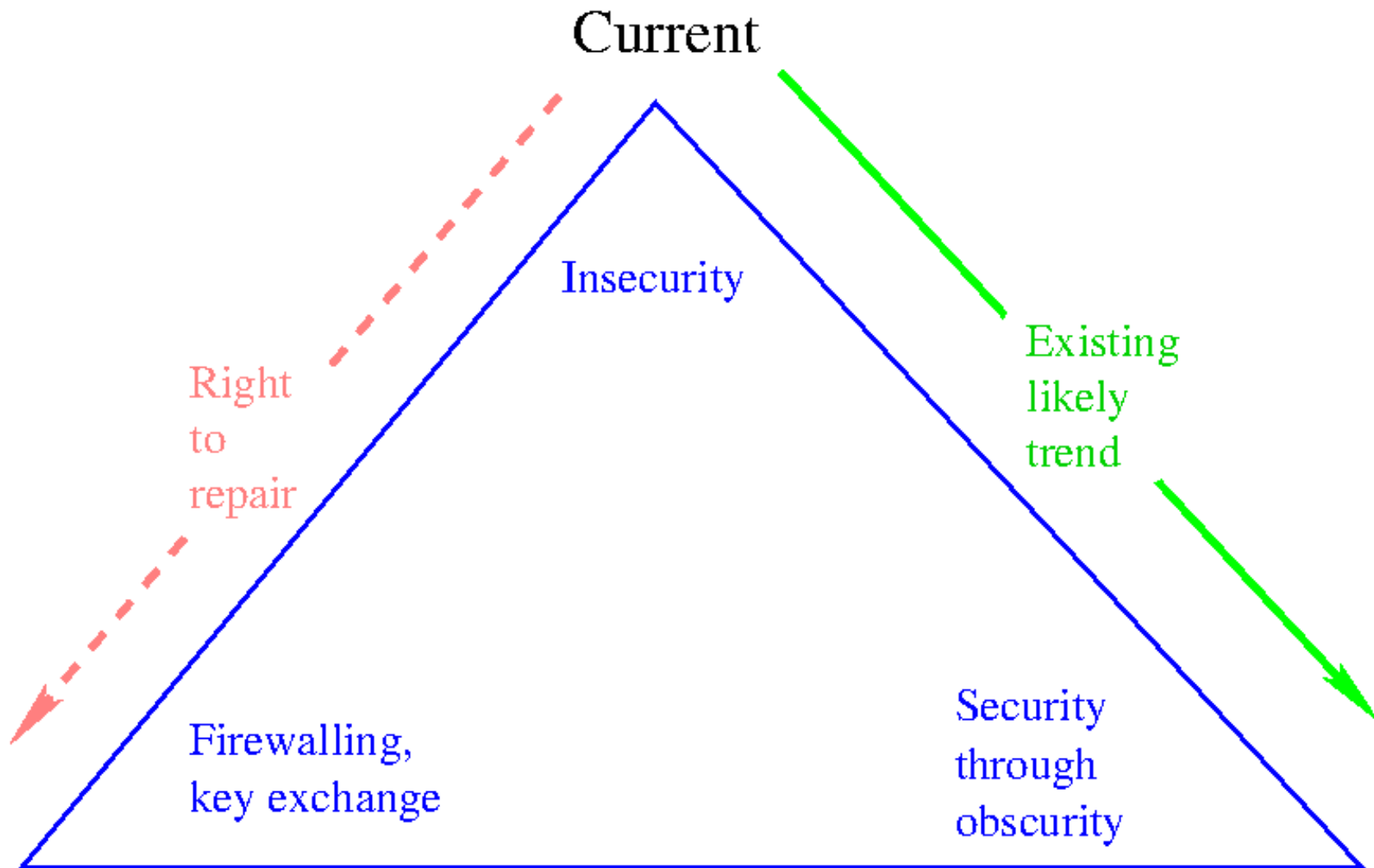


Published UWa/UCSD automotive exploit

<http://www.autosec.org/>

- Use Gnu Radio to break in via wireless tire pressure sensors.
- Discover all of 8-byte codes by “fuzzing” attack.
- Or simply watch bus traffic to get many.
- Brakes locked and driver controls disabled via use of codes or simple DOS attack.
- But let's not make instrumenting ***our own*** vehicles illegal, too!

Free culture movement needs to get involved in automotive



How to fix automotive security

- Automotive network protocols genuinely do need to be hardened.
- Packet filtering, firewalls, cryptographic signing and Android “paranoid network” exist.
- Any approach that posits the necessity to invent new technologies is *wrong*.
- If NHTSA promulgates new rules, EFF, FSF, SFLC should participate!

FSF is on the vanguard again

June 23, 2011, 1:01 PM

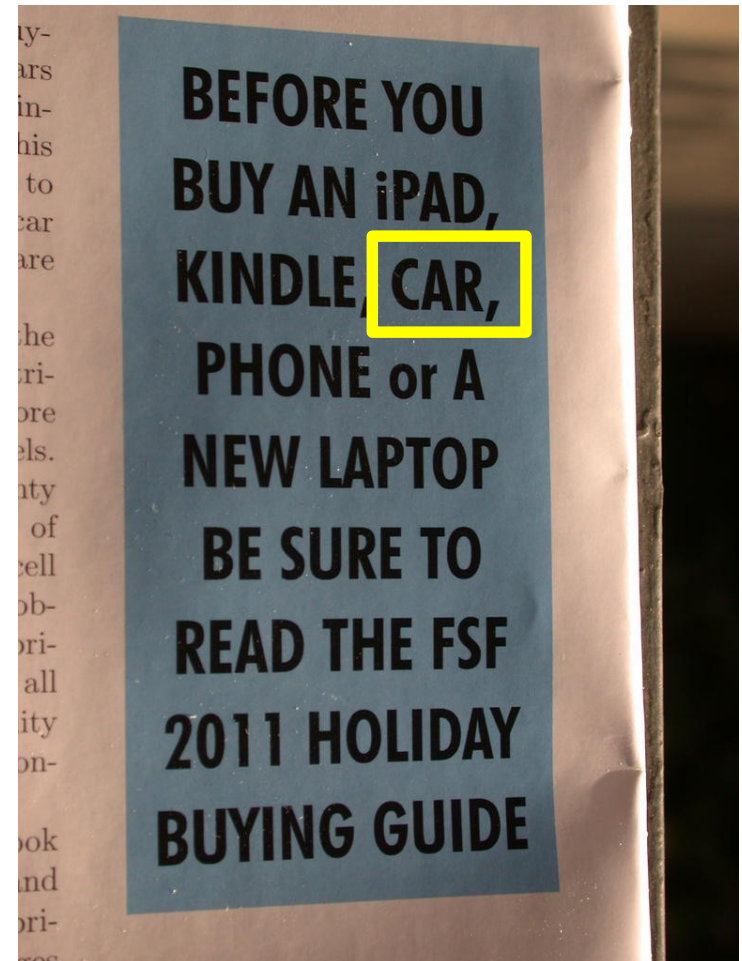
'Aggravating' MyFord Touch Sends Ford Plummeting in J.D. Power Quality Survey

By CHERYL JENSEN



The MyFord Touch interface as seen on the 2011 Ford Edge.

New York Times, June 23 2011



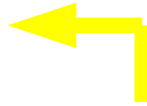
Ongoing mobile data privacy battle

“For crashes that don't involve litigation, especially when police or insurers are interested in assessing fault, insurers may be able to access the EDRs in their policyholders' vehicles based on provisions in the insurance contract requiring policyholders to cooperate with the insurer. However, some states prohibit insurance contracts from requiring policyholders to consent to access.”

Source: Insurance Institute for Highway Safety,
<http://www.iihs.org/research/qanda/edr.html>

Privacy Guarantees in Car Environment

- JM1BK3437512345678



Vehicle Identifier Section: a particular car

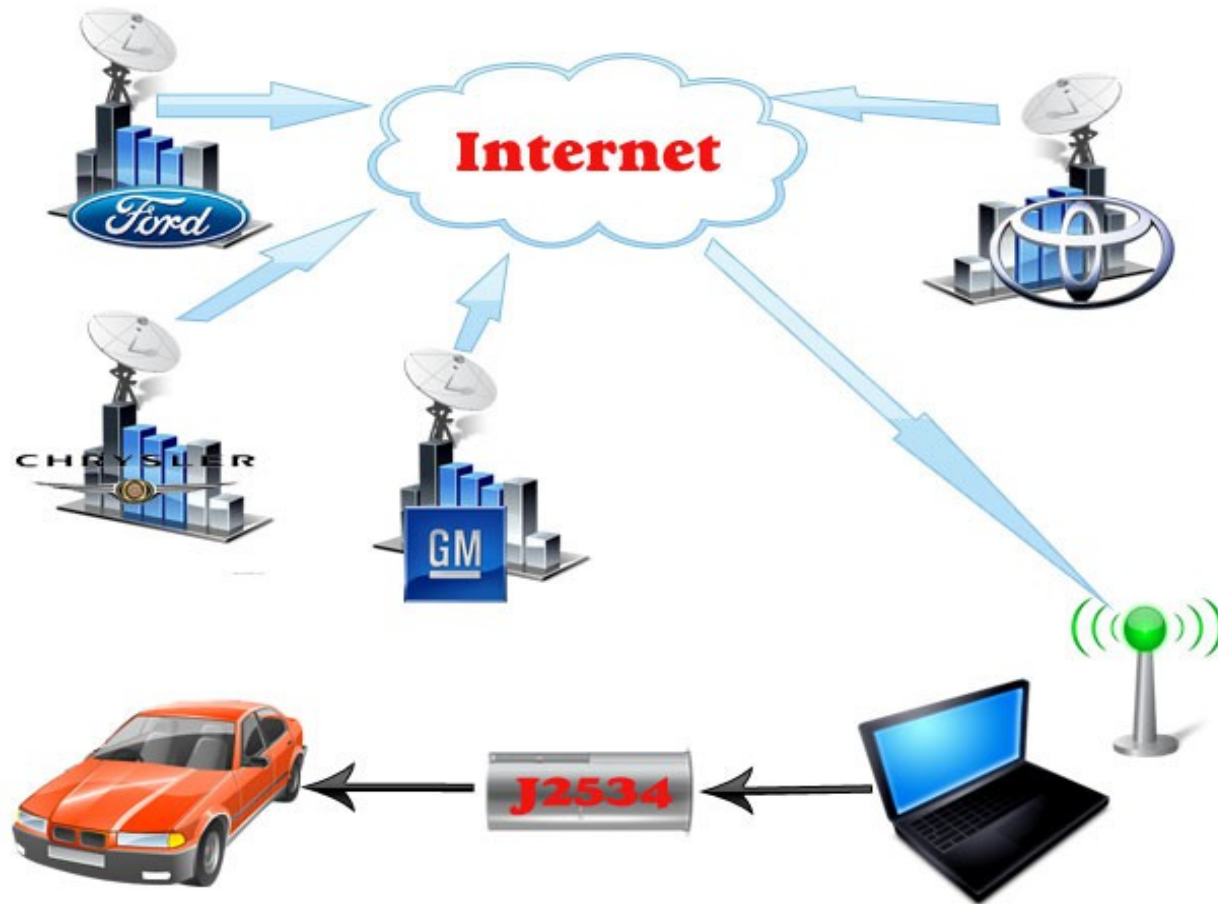
- *Proposal*: encrypt the Vehicle Identifier Section of the VIN so that it cannot be remotely transmitted.
- Require “apps” to request access to VIS.

Motor Vehicle Owners Right to Repair Act

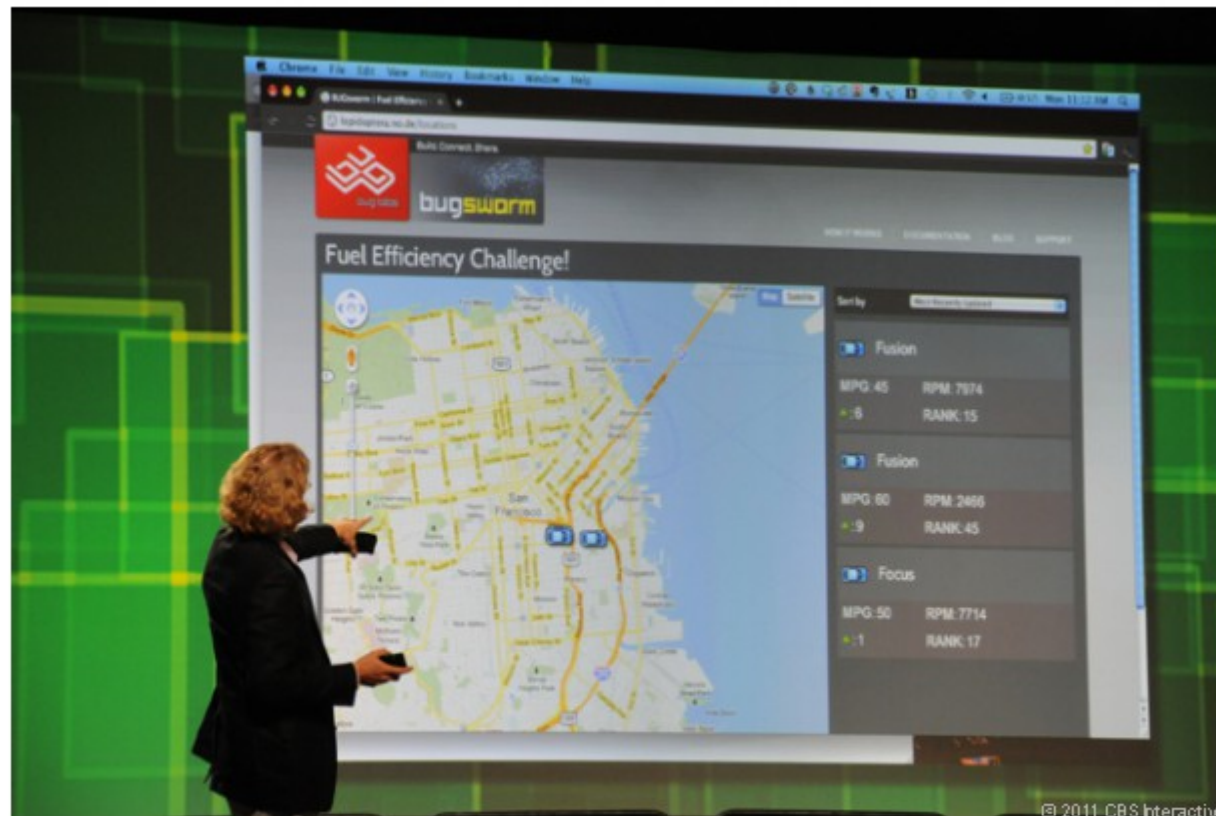
... requires vehicle manufacturers to provide the same service information to *independent shops* that they offer to their franchised dealers. Under current law, auto manufacturers protect their proprietary vehicle repair information, requiring consumers to bring their cars to the dealer for expensive repairs. The bill allows independent mechanics to compete fairly with dealerships in providing repair and maintenance services ...

Source: Congresswoman Anna Eshoo

MA “Right to Repair” Initiative 2012



Vehicle data example: Ford's Fuel Efficiency Challenge



As part of its OpenXC announcement, Ford and Bug Labs showed off the Fuel Efficiency Challenge, which allows drivers of Ford Sync-enabled cars to share their fuel efficiency with others.

(Credit: Daniel Terdiman/CNET)

Some owner-empowering vehicle-data-mining ideas:
<http://tinyurl.com/7oegrj7>

Quality community-sourced hardware and software already available



<http://tinyurl.com/7wngdsj>, <http://tinyurl.com/7ttz24h>

CFR PART 563—EVENT DATA RECORDERS

“Each manufacturer of a motor vehicle equipped with an EDR shall ensure by licensing agreement or other means that a tool(s) is commercially available that is capable of accessing and retrieving the data stored in the EDR that are required by this part. The tool(s) shall be commercially available not later than 90 days after the first sale of the motor vehicle for purposes other than resale.”

source: NHTSA website

What does it mean to “own” data?

The creator of the device that generates data that I own ***must*** provide, as a bare ***minimum***

“any methods, procedures, authorization keys, or other information required” to read the data

and

“information provided [. . .] must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.”

Free software community responds to embedded challenges

ZDNet / Open Source / Story

Cyborg lawyer demands software source

By Stilgherrian, ZDNet.com.au on January 20th, 2012 [Follow @stilgherrian](#)



Eben Moglen SSCL lecture 2010

by Robert McWilliam
1 year ago



Summary

- Old battles are renewed in new arena.
- Proprietary interests will deny device owners access to their data with the excuse of protecting public safety.
- Proprietary interests will claim that security by obscurity is better than proven network security standards.
- Engineering implementers need the wise counsel of those who understand the Law.