Your Car's Data is Showing: Privacy in the Age of Connected Cars
Use the Automatic
During the Convention

Make the Automatic Telephone Station at the Coliseum your headquarters. A reception room, booths and uniformed pages at your service on the main floor of the Annex.

Let us facilitate your work—and let us demonstrate to you the wonderful efficiency of the Automatic telephone—

The ONE Phone That Gives SECRET SERVICE

Automatic Telephone Service is pulling the biggest popular vote in history! Local Chicago traffic has more than doubled, and long distance increased 80%; since January 1, 1912.

Because of its very low cost, its instantaneous connections, its accuracy, its splendid carrying power, the Automatic is the only logical telephone. By all means take advantage of this special convention service.

Local Calls 5c
Long distance calls at remarkably low rates

Illinois Telephone & Telegraph Co.
(Successor to Illinois Telerat Co.,
Telegraph Department)
162 W. Monroe St.
Commercial Dept.
33-111
Information 899
Long Distance
Call (O) on the Dial

AUTOMATIC
1991: California Air Resource Board requires OBD

1994: OBD-II specification is finished

1996: Mandatory for all cars manufactured in the United States
Drive Smarter
Drive Safer
Connect your car to the internet of things
What does your car say about you?
OBD II
Information we Collect

- GPS readings
- Battery voltage, check engine light and codes.
- Speed, RPM, fuel-injection rate, fuel level and hundreds of other car sensors every second.
<table>
<thead>
<tr>
<th>mpg above sticker</th>
<th>car model</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6</td>
<td>– 2010 Nissan Maxima S</td>
</tr>
<tr>
<td>0.6</td>
<td>– 2012 Nissan Frontier SV</td>
</tr>
<tr>
<td>0.2</td>
<td>– 2011 Toyota Tacoma Base</td>
</tr>
<tr>
<td>0.0</td>
<td>– 2012 Toyota Corolla L</td>
</tr>
</tbody>
</table>

- 2013 Subaru Impreza Sport Premium
- 2014 Jeep Grand Cherokee Overland
- 2011 Hyundai Sonata GLS
- 2012 Subaru Impreza Sport Limited
- 2013 Nissan Altima SV
ISO 11898-3 Network
May Be Bus, Star, or Mixture
OBDII Hacks Leave Vehicles Vulnerable

January 26, 2015 / 0 Comments / in Blog / by Pwnie Express

Modern vehicles pack a considerable amount of processing power, and with self-driving vehicles on the horizon, they are only going to get “smarter” in the near future. There’s been talk of security vulnerabilities with modern computerized vehicles in the past, but they’ve largely been a topic of time poring over.

But recent research has shown that millions of drivers to report problems with all vehicles with the device installed, and in fact, vehicle cyber attacks present a serious threat.

**Hacking the Zubie**

The most detailed research in analyzing the cellular modem and automating a common serial UART. After connecting the serial up to their computer, the researchers were presented with a command interface that allowed them to download all the files stored on the device. After decompiling the Python files that make up the interface, it was possible to start exploiting the device.

**Hacker Says Attacks On 'Insecure' Progressive Insurance Dongle In 2 Million US Cars Could Spawn Road Carnage**

+ Comment Now  + Follow Comments
hackers remotely kill a jeep on the highway—with me in it
HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET
Automakers Say You Don’t Really Own Your Car

EFF is fighting for vehicle owners' rights to inspect the code that runs their vehicles and to repair and modify their vehicles, or have a mechanic of their choice do the work. At the moment, the anti-circumvention prohibition in the Digital Millennium Copyright Act arguably restricts vehicle inspection, repair, and modification. If EFF is successful then vehicle owners will be free to inspect and tinker, as long as they don’t run afoul of other regulations, such as those governing vehicle emissions, safety, or copyright law.

You can support EFF’s exemption requests by adding your name to the petition we’ll submit in the rulemaking.

Most of the automakers operating in the US filed opposition comments through trade associations, along with a couple of other vehicle manufacturers. They warn that owners with the freedom to inspect and modify code will be capable of violating a wide range of laws and harming themselves and others. They say you shouldn’t be allowed to repair your own car because you might not do it right. They say you shouldn’t be allowed to modify the code in your car because you might defraud a used car purchaser by changing the mileage. They say no one should be allowed to even look at the code without the manufacturer’s permission because letting the public learn how cars work could help malicious hackers, “third-party hackers who want to break into your car.”
Allow Concur to access your car data?

- Concur will never access your password.

- Driver profile
- Real-time location
- Basic car information
- Vehicle identification number
- Trips and routes
- Your driving behavior
- Diagnostics
- Streaming data while you drive

- Don’t Allow
- Allow
14 HARD ACCELERATIONS

Slamming on the gas is risky and doesn’t save much time.
Consider leaving plenty of room between you and the car in front to avoid braking hard.

2 HARD BRAKES

Though sometimes hard to avoid, slamming on the brakes is linked to risky driving.
Consider leaving plenty of room between you and the car in front to avoid braking hard.

56 LATE-NIGHT DRIVING MILES

Accidents are more likely between midnight and 4am when drowsy drivers are on the road.
Stay focused, and if you can, avoid driving during these times.

452 MILES DRIVEN

People who drive less are at lower risk of accidents, and may earn a larger discount.
Bay Area’s riskiest on-ramps keep hearts racing

By Evan Sernoffsky  Updated 1:04 pm, Friday, February 20, 2015