This vehicle allows access to telematics services that require collecting and transmitting data, for processing by Nissan Motor Co., Ltd., related to the battery storage capacity, your driving efficiency and in limited cases, your vehicle location. Full details are in the owner's manual.

Touch OK to accept.

OK  Decline
PRIVACY IMPLICATIONS OF INTELLIGENT TRANSPORT SYSTEMS

Khalil El-Khatib
Rajen Akalu
Kushal Jaisingh
THE JOURNEY

- Technology is rapidly advancing in the transport sector
TODAY’S CONNECTED VEHICLES

- Modern vehicles
  - More than 50 networked computers:
    - Average new vehicle has 40 to 50 computers that run 20 million lines of software code, more than a Boeing 787 (KPMG)
  - Networks on wheels
- Infotainment and telematics systems generate, collect, and transmit lots of data to provide on-board features for a safe and comfortable ride!!!
- Contains potentially sensitive information about driver!
TODAY’S CONNECTED VEHICLES

- New vehicles have many sensors and have multiple options to connect to other types of networks
- Gather and generate lots of data to provide on-board features to consumers
  - Contains potentially sensitive information about consumers
  - Remotely accessible by automakers and infotainment/telematics service providers
BACKGROUND – INFOTAINMENT SYSTEMS

- Contain non-vehicular information
- Provide drivers convenient onboard functions when driving:
  - Hands free calling
  - Text messaging
  - Emailing
  - ...
BACKGROUND – TELEMATICS SYSTEMS

- Contain vehicular information about vehicle’s internal systems
- Primarily used for vehicle diagnostics and emergency situations to automatically provide roadside assistance service providers pertinent information
VEHICLE IDENTIFICATION DATA INCLUDES

- Vehicle identification number (VIN)
- Subscriber identify module card number (SIM)
- Internet protocol address (IP)
- Radio frequency identification serial number (RFID)
  - Many vehicles are equipped with RFID tags for toll collection, and can be linked to vehicle owners’ billing account information for their toll usage
  - Some vehicle keys contain embedded RFID tags for convenience and personalization of drivers’ seat settings
- Can be used to reveal the identity of the owner of the vehicle
PERSONAL INFORMATION

- Personal information is “information about an identifiable individual”
- Includes identification data, personal communications data, biometric and health data, location data, driver behavior data, and miscellaneous infotainment data
- Driver behavior data and miscellaneous infotainment data aren’t considered personal information, but certainly have implications on one’s privacy
† Includes:
  † Voice calls
  † Text messages
  † Emails
  † Social networking information
Each personal communication event’s data is accompanied by its corresponding metadata including:

- Event’s date
- Time
- Origin
- Destination
- Duration
- ...

PERSONAL COMMUNICATIONS DATA - METADATA
Some vehicles contain biometric authentication and health monitoring devices.

Information retrieved from these devices can also reveal the identities of drivers.
DRIVER BEHAVIOR DATA

- Includes information regarding drivers’ driving habits such as vehicle speed, acceleration, direction, braking, cornering, ignition, steering, seat belts, and door locking
- Alone cannot be used to identify individuals
- Combined with vehicle identification data, could have major privacy implications
VEHICLE LOCATION DATA

- Includes recently visited destinations as well routes travelled
- Alone may not be able to reveal identities of individuals
- Combined with other data sources, major privacy implications arise as intimate details of individuals’ private lives are portrayed
MISCELLANEOUS INFOTAINMENT DATA

- Includes personal contacts, calendar/planner schedules, search history, recently viewed content (photos, audio, video, websites), and any other data which may be synced from mobile devices
- Reveals a lot about individuals’ personal lives
- Can be used for profiling individuals based on their social associations, interests, and content preferences
DATA USAGE IN INFOTAINMENT AND TELEMATICS SYSTEMS

- Live agent assistance, including:
  - Automatic collision notification emergency assistance
  - Roadside assistance

- Remote monitoring and control, including:
  - Remote vehicle diagnostics
  - Fleet management
    - Can monitor vehicle location and routes travelled in real time including vehicle speed and driving violations
  - Usage-Based Insurance (UBI)
  - Automotive financing
• **Geo-fencing**
  • Used in fleet management and automotive financing applications to confine vehicles to a specific predefined geographic boundary
  • If vehicle roams out of its boundary, predefined actions are executed such as:
    • Notify fleet manager or financier of boundary breach
    • Remotely disable vehicle

• **Location-based advertising, including:**
  • Vehicle-to-Retail (V2R) location-based advertising communications are targeting drivers
  • GM’s “AtYourService” feature allows their business partners to notify OnStar subscribers of special offers
DATA USAGE IN INFOTAINMENT AND TELEMATICS SYSTEMS

• Distance-based road taxation
  • Provides drivers the option to either pay a high flat rate for unlimited driving on toll roads
  • Or a lower rate based on the GPS data collected by a voluntary dongle or mobile app which monitors the distance travelled on the toll roads

• Electronic tolling
  • Relies on roadside RFID scanners and Automatic License Plate Readers (ALPRs)
  • Scans vehicles’ RFID tags and license plates as they pass through entry and exit nodes of toll roads to determine the amount owed
Personal Connectedness and Infotainment, including:
- Include hands-free communications via voice commands for drivers to safely engage in communications
- Contacts, calendar data, and other information is automatically synced to the vehicle to provide infotainment services
THIRD PARTY INTERESTS

▪ Infotainment/telematics data has become a very hot commodity
▪ Many people are interested in purchasing this data for the valuable insights it can provide using data analytics
THIRD PARTY INTERESTS - TOMTOM

- TomTom was caught selling customer GPS data to ___ ______ ___ for creating speed traps
- Dutch law enforcement
Ford’s Global VP of Marketing said:

- “We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing”

He later clarified his statement by saying:

- “We do not track our customers in their cars without their approval or consent”

Despite his clarification, automakers still have the ability to track their customers’ vehicles and mine sensitive information.
POTENTIAL PRIVACY VIOLATION – GM’S ONSTAR

- GM’s OnStar service provides directions, roadside assistance, and concierge services to its subscribers.
- Recently, GM added their new AtYourService feature to their existing OnStar service offerings.
Let us find ourselves what is on these systems

- What is stored on these systems and how can it be used to determine information about its users?
TARGET SYSTEMS

- Many car manufacturers
- Many different platforms: Ford SYNC, Dodge uConnect, GMC/Chevrolet OnStar/MyLink, etc.
- Different generations among same branded platforms (e.g. SYNC Gen1, Gen2)
- Windows, Linux/Android, QNX based systems
- Aftermarket systems → same case as above (Android more popular)
DATA ACQUISITION PROCESS

- Not as straightforward as initially thought...especially car manufacturer
- Not everyone is willing to let us take their vehicle apart for one main component
- Original Equipment Manufacturers (OEMs) are complicated to power up standalone but represent majority of market
FORD F150 TRUCK

- Based off this first dump, lots of relevant information stored!
- Logs upon logs upon logs
- GPS breadcrumbs
- Phonebook folder
- Web browsing folder (nothing in it but feature might not of been used)
- Etc.
MORE HARDWARE

- At this point, need to do more investigation
- Plan: acquire more infotainment systems
- Contacted junkyards and dealerships
- Turns out powering up the system standalone isn’t as straightforward as aftermarket systems... entire wire harnesses, vehicle fuse box and Body Control Module (BCM) needed
- Process of acquiring and wiring up one Ford SYNC platform took almost a moth (trial and error and finding out components were missing before it could work)
Alright, now that we have some hardware, how are we extracting the data??!?
• iVe (forensic software specifically for OEMs used in conjunction with hardware extraction)

• Supports BMW, Buick, Cadillac, Chevrolet, Chrysler, Dodge, FIAT, Ford, GMC, HUMMER, Jeep, Lincoln, Maserati, Mercury, Pontiac, Ram, SRT, Saturn, and Toyota (generally 2008 and up)

• Only one problem... licence is ridiculously expensive
IN THE MEANINGLEM... 

- Curious about what could be found on vehicles through simple user interactions
- OWASCO Volkswagen/Audi dealership willing to help us with second-hand vehicles on lot
- Are users aware of what they could be leaving behind?
VEHICLES

- 2013 VW Passat (no GPS, just basic infotainment)
- 2014 VW Touareg (higher end infotainment with GPS)
- 2012 Audi Q5 (higher end infotainment with GPS)
- 2014 Audi Q7 (higher end infotainment with GPS)
OBSERVATIONS

- Bluetooth device lists (profiles)
- Phone contacts
- Profile information (name, device info, # of imported contacts)
- Navigation info and addresses still stored including exact coordinates
- Can export contacts/GPS information to SD/USB (any that were imported, depending on system)
Decided to acquire aftermarket systems as they’re still relevant in the market

- Windows CE 6 based infotainment (OUKU brand)
- Android Kitkat 4.4.4 infotainment (Pumpkin brand)
- Android variant with Android Auto and Apple Carplay (Pioneer brand)
DATA EXTRACTION PROCESS

- Basically, these were using commonly available operating systems so much more straightforward
- Gain SU and enable debugging mode or even better, get a terminal session going (especially for Android)
- Once complete, dd all the sectors into an .img file
- For Windows CE, replace GPS.exe shortcut with another .exe (explorer.exe in this case then full admin rights)
Ford SYNC infotainment systems seem to keep all contacts, phone profiles as well as Bluetooth addresses and filesystem items.
phones with Jeep UConnect
Caught on webcam, burglars hunted on social media with help from phone names.

by Sean Gallagher - Feb 11, 2016 11:44am EST
@baconisfruit's car gets stolen. Criminal geniuses pair their phones' Bluetooth. #OPSECfail (OSINT @AmazinMojoStarz)
LAWS, POLICIES, AND USERS

- Previous law and policy research has demonstrated a widespread disrespect for the privacy of customers by companies offering connected car services.

- Survey research indicates that drivers will be more comfortable with the use of connected systems if they have some measure of control over their privacy settings.
LAWS, POLICIES, AND USERS

- Apart from PIPEDA, there are no laws enforced to limit the collection and use of customer information by automakers.
- Customers must trust the policies and terms dictated by automakers and infotainment/telematics service providers.
WHAT DID WE CONCLUDE?

- Privacy policies are a necessary but an insufficient form of privacy protection in the connected vehicle context.

**Necessary because...**
- Privacy regulation is based on the notion that the individual ‘data subject’ exercises control over their personal information
- It is also a consent driven model

**Insufficient because...**
- People do no read privacy policies
- People over value the immediate benefits obtained from revealing personal information and under estimate the cost of privacy loss
- Companies often use privacy policies to seem trustworthy while mitigating unethical data handling practices
RECOMMENDATIONS FOR REFORM

- Design for Privacy
- Only collect data required to provide the original service advertised (not secondary purposes such as marketing).
- Only access and use the data collected for purposes involved with providing the advertised service.
- Do not share collected data with third-parties even if data is de-identified unless required for the service.
RECOMMENDATIONS FOR REFORM

• Ensure “Terms and Conditions” and “Privacy Policy” documents clearly identify what data will be collected from both infotainment AND telematics systems, as well, define how the collected data will be used.

• Collected data should only be retained for the duration required by the service and then securely erased.

• Should a company choose to employ a less strict version of the policies recommended above which shares customer information with third-parties, customers should be provided the option to opt-out on the spot and their request should be processed immediately; preventing customer information to be shared starting from the time their service begins.
ADDITIONAL PRIVACY RECOMMENDATIONS FOR CAR DEALERS AND RENTAL COMPANIES

- Ensure any existing data from both the infotainment AND telematics system is cleared prior to selling/renting the vehicle.
- Employ vehicle inspection reports to verify that the data has been cleared.
INDEPENDENT CREDENTIALING AUTHORITY

- Trusted by customers, manufacturers, system operators, service providers
- Created by statute.

Establish rules for:
- Initialization – Vehicle set-up
- Operation – Major mode of operation
QUESTIONS?