

July 31, 2017

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue N.W., Suite CC-5610 (Annex A)
Washington, DC 20580

Re: Follow-up Comments for the FTC/NHTSA “Connected Cars – Workshop, Project No. P175403

The Center for Democracy & Technology (CDT) was pleased to contribute to the joint workshop on privacy and security in connected cars held by the Federal Trade Commission (FTC) and the National Highway Traffic Safety Administration (NHTSA). In light of our participation in that workshop and continuing policy movement in the automotive ecosystem, we submit these additional comments to highlight observations regarding notice, data security, and data sharing by automakers.

The connected vehicle ecosystem consists of a growing network of automakers, telecom companies, telematics service providers, insurance companies, and a host of other players sprawled across disparate distribution channels.¹ To add to an already crowded landscape, automakers are proactively harnessing partnerships with AI developers and ride-sharing companies,² as well as entertainment and social media companies like Facebook that are eager to have an in-vehicle presence.³

At the same time, there have been growing calls for a more cautious and measured approach to increasing online connectivity and vehicle data sharing. We applaud the FTC and NHTSA’s recent workshop, and more recently, were pleased to see a number of important privacy and security provisions including in bipartisan legislation that passed out of the House Energy and Commerce Committee to facilitate autonomous vehicle deployment. For example, the SELF DRIVE Act requires the preparation of written privacy plans, the formation of a Highly Automated Vehicle Advisory Council, and envisions further reports by the FTC.⁴

We note that the FTC/NHTSA workshop addressed a variety of unique concerns raised by connected vehicles, but that commentators’ predominant focus was on vehicle cybersecurity. To their credit industry players have demonstrated a degree of proactivity and willingness to address these risks. Automakers, or original equipment manufacturers (OEMs), now share security information through the Automobile Information Sharing and Analysis Center (Auto-ISAC). However, there is still a long way to

¹ See Liz Slocum Jensen, This is the Connected Car, VB Profiles (Apr. 2016), <https://www.vbprofiles.com/l/connectedcarstwitter>.

² See e.g., D. Etherington, GM Puts IBM Watson in Cars with the New OnStar Go Platform, TechCrunch (Oct. 26, 2016), <http://tcrn.ch/2f6X4Cy>; D. Etherington, Toyota and NTT to collaborate on connected car tech, including AI, TechCrunch (Mar. 27, 2017), <http://tcrn.ch/2m1ZQRG>.

³ See J. Butters and S. Frier, Facebook is Determined to Build Ties with Automakers, Bloomberg Technology (Jun. 8, 2017), <https://www.bloomberg.com/news/articles/2017-06-08/facebook-s-detroit-status-feeling-determined-to-build-auto-ties>.

⁴ See Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act (“SELF DRIVE Act”), H.R. 3388, <http://docs.house.gov/meetings/IF/IF00/20170727/106347/BILLS-115-HR3388-L000566-Amdt-9.pdf>.

go. As we noted in our previous comments to the FTC and NHTSA motor vehicle security research is still in its infancy, and the public lacks any meaningful insight into automakers' data security practices.⁵

Better transparency will be a key driver to improving consumer trust in the connected car ecosystem. As the workshop reiterated, the 2014 Automotive Privacy Principles emphasize transparency as a primary mechanism for detailing OEMs' commitment to consumer privacy protections, with a focus on exploring a variety of methods to provide clear, meaningful notices.⁶ However, in the near three-year period since the adoption of the Privacy Principles, it continues to be unclear how far automakers have moved beyond traditional notice and consent principles to improve transparency for consumers. CDT encourages the OEMs to work together to promote standardized privacy and security disclosures under the Privacy Principles; in particular, we suggest a focus on defining the baselines for data security, notice mechanisms, and sharing with law enforcement.

In order to offer concrete guidance to the industry in these areas, CDT has teamed up with the Usable Privacy Policy Project at Carnegie Mellon University (CMU)⁷ to examine one narrow area of the connected car ecosystem: the mobile apps provided by OEMs to facilitate driver access to information on or about their vehicles. Through a combination of natural language processing and static analysis, the CMU team built the Mobile App Compliance System (System). The System is designed to review mobile app privacy policies and compare those disclosures against each app's actual data use, collection and sharing practices based on an analysis of the app's code.⁸ We tested a total of 32 Android mobile apps offered by the 19 automaker signatories to the Privacy Principles.⁹ The System yielded key insights into areas for improvement in notice and transparency, raising the potential utility of technical solutions that users and regulators alike can leverage to manage the growing connected cars economy.

1. Data Security

The Privacy Principles include a commitment to securing user information against unauthorized access or use. As currently written, this requirement is not detailed and only requires a commitment to "implementing reasonable measures" and that "[r]easonable measures include standard industry practices," with the recognition that those standards should evolve in accordance with emerging threats and vulnerabilities over time.

As a result, data security provisions in OEM privacy policies are oftentimes scant and provide little information about the actual security measures in place to protect consumer information. Rather, the

⁵ Comments of the Center for Democracy & Technology (Apr. 28, 2017), <https://cdt.org/files/2017/05/CDT-FTCNHTS-A-Connected-Cars-Submission.pdf>.

⁶ Alliance of Automobile Manufacturers, Inc. & Association of Global Automakers, Inc., *Automotive Privacy*, <https://autoalliance.org/connected-cars/automotive-privacy-2/> ("Automotive Privacy").







⁷ The Usable Privacy Project is a National Science Foundation project, led by Professor Norman Sadeh at Carnegie Mellon University, available at <https://www.usableprivacy.org>. CDT thanks Professor Sadeh, along with Dr. Sebastian Zimmeck, Peter Story, Ziqi Wang, and Sushain Cherivirala for their technical expertise and collaborative efforts in using the Mobile App Compliance System's capabilities for CDT's connected vehicles analysis.

⁸ Specifically, the System downloads Android Package Kit (APK) files from the Google Play Store and then conducts a static analysis of the downloaded APK. This analysis includes extraction of app permissions and evaluation of first and third party use of Android APIs to assess what data types are collected by the app publisher and shared with which third parties. The System is not currently publicly available.

⁹ A complete list of mobile apps that the System analyzed is available in **Appendix A**.

policies provide standard boilerplate statements, providing that “[w]e maintain reasonable and adequate security controls to protect your information and require our service providers by contract to do the same,”¹⁰ or that “[w]e have appropriate technical, administrative and physical procedures and information security policies in place to safeguard your information from loss, misuse, or alteration.”¹¹ These vague statements provide limited insight into the OEM’s actual data practices and require consumers to trust that reasonable protections are in place.¹²

In this context it is noteworthy that CMU’s System found that while a majority of apps encrypted their communications, several mobile apps – 12.5% – seem to engage in the *unencrypted* transmission of location and other sensitive information. While this limited information makes it impossible for us to know if encryption is needed for these types of communications, it highlights the need for further clarity as to what should be the norm.

| Static Analysis Practice ⓘ | HTTPS | Third Parties ⓘ | App Permissions |
|--|-------|-----------------|---|
| Location WiFi 1st Party  </> 8 Segments | No | | ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, INTERNET |
| Location GPS 1st Party  </> 48 Segments | No | | ACCESS_FINE_LOCATION, INTERNET |
| Location Cell Tower 1st Party  </> 8 Segments | No | | ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, INTERNET |
| Contact ZIP 1st Party  </> 11 Segments | No | | INTERNET |
| Contact Postal Address 1st Party  </> 8 Segments | No | | INTERNET |
| Contact City 1st Party  </> 11 Segments | No | | INTERNET |

Screenshot: Carnegie Mellon University Mobile App Compliance System, showing static analysis of one mobile app that seems to fail to use an HTTPS connection to collect and transmit Location and certain Contact information.

¹⁰ General Motors, OnStar Privacy Statement, <https://www.onstar.com/us/en/footer-links/privacy-policy.html> (last updated Jan. 1, 2017).

¹¹ NissanConnect, Privacy Notice, <https://www.nissanusa.com/connect/privacy> (last updated Dec. 2015) (“Nissan Connect Privacy Notice”). See also Subaru Starlink, Privacy Policy, <http://www.subaru.com/company/starlink-privacy.html> (last updated Apr. 7, 2016) (“Subaru Starlink Privacy Policy”).

¹² Furthermore, these data security provisions often include a blanket caveat acknowledging general security vulnerabilities in network systems and discounting any liabilities thereof. See *id.* See also Ford SYNC, Terms & Conditions of Use, <https://owner.ford.com/tools/account/sync-terms-and-conditions.html> (last updated Aug. 3, 2016); Toyota Connected Vehicle Services, Privacy and Protection Notice, <https://www.toyota.com/privacyvts/images/doc/privacy-portal.pdf>.

Generally OEMs would better serve consumer interests by providing more detailed disclosures of their data security practices. Of course this would not preclude companies from working together to proactively define what constitutes standard industry practice. However, more detailed disclosures would, in theory, allow consumers to better compare and contrast statements across different companies and make their own decisions about whether each company is measuring up to that industry standard. A practical starting point might include a commitment to the use of encrypted connections wherever consumer information is transmitted. As the FTC’s Staff Internet of Things Report¹³ acknowledges, the interception of unencrypted data transmissions is a significant concern in the Internet of Things. OEMs have a unique opportunity to be a leader in providing more education and transparency into reasonable security measures.

2. Transparency and Notice

Transparency and better notice mechanisms are considered by the Privacy Principles as key priorities to improving consumer awareness and trust. The Association of Global Automakers reiterated this in its comments to the FTC/NHTSA workshop, in which they stated the “Privacy Principles are rooted in transparency and consumer choice.”¹⁴ Workshop panel discussions also echoed this point in recognizing a need for continued consumer education and better ways to communicate with the consumer, such as through onboard mechanisms to detect cybersecurity intrusions and system updates.

For now, the industry remains largely dependent on the notice-and-consent regime to effectuate transparency. The last twenty years have demonstrated the limitations of a notice-and-consent regime.¹⁵ In this case, this reliance on pure disclosure principles places the onus on individual consumers to become fully informed of each OEM’s data practices, not to mention those pertaining to a growing network of affiliated partners and service providers. Many OEMs further obligate their consumers to inform and obtain consent from any passengers and non-owner/lessee drivers before engaging in the connected car services. For instance, one OEM’s telematics subscription agreement provides that a consumer’s consent to its terms is “for yourself, your Vehicle’s occupants and anyone contacting us on your behalf.”¹⁶ Considering that even the most sophisticated OEMs find it difficult to effectively communicate privacy information, unilaterally placing this responsibility on individual consumers is certainly asking for too much.

Worse, our review of automotive apps found that of the 32 apps tested, a third did not contain a link to the correct privacy policy. In most of these cases, the links were to the OEM’s website privacy policy, which are not specific to the connected service mobile app. In other cases, the correct policy was incorporated into the general policy as a hyperlink. This sort of embedded “see more” function runs the

¹³ Fed. Trade Comm’n, FTC Staff Report on *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

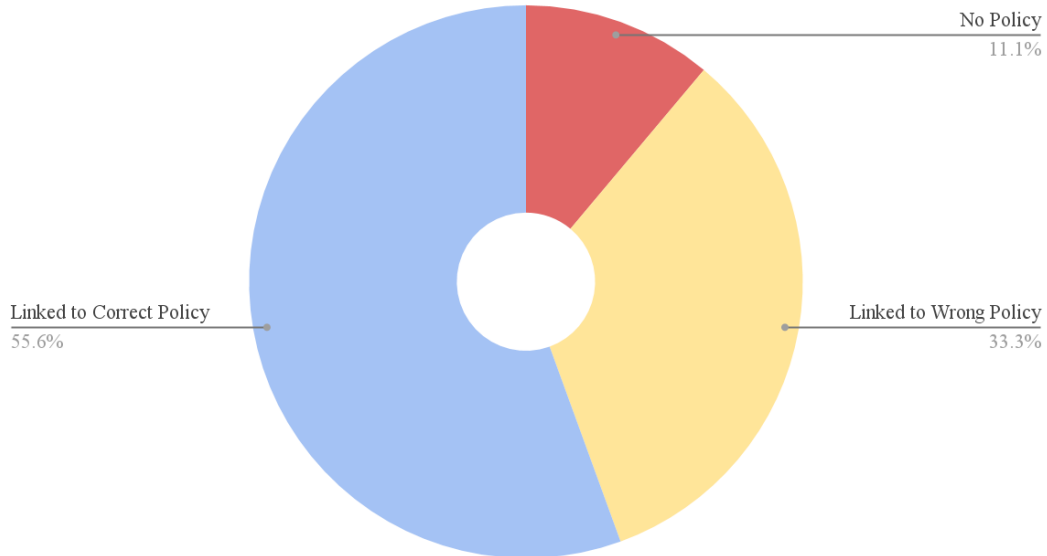
¹⁴ Comments of the Association of Global Automakers, at 4 (May 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/05/00041-140624.pdf.

¹⁵ See Shankar Vedantam, *To Read All Those Web Privacy Policies, Just Take A Month Off Work*, NPR (Apr. 19, 2012), <http://www.npr.org/blogs/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacypolicies-just-take-a-month-off-work>.

¹⁶ Toyota Entune, Telematics Subscription Service Agreement, <https://www.toyota.com/privacyvts/images/doc/Toyota%20SSA.pdf> (last updated Jun. 2017). See also NissanConnect Privacy Notice, *supra* at 11; Subaru Starlink Privacy Policy, *supra* at 11.

risk of consumers missing it entirely, and at the very least, adds to the consumer’s burden of becoming informed.

Figure 1. CMU System Analysis of Privacy Policies



As Figure 1 shows, the CMU System also found that 4 apps did not have a privacy policy at all, either in the Google Play Store or within the app itself. The static analysis for each of these apps shows collection of personally identifiable information, suggesting possible violations of state privacy laws, including the California Online Privacy Protection Act,¹⁷ as well.

Companies like Toyota have taken a step towards centralizing the information into an online privacy portal,¹⁸ and this is an easy first step that all OEMs can adopt. Looking forward, OEMs should also consider adapting their UI/UX expertise, often used to create intuitive and appealing dashboards, to developing more visceral and integrated notices into the natural driving experience.¹⁹ These efforts should also contemplate the provision of more *opportunities* for consumers to review their privacy preferences, as opposed to the single request for perpetual consent prior to initial collection.

3. Data Sharing with Law Enforcement

The Privacy Principles recognize that in order to build strong data protections and maintain consumer trust, automakers need to “clearly state the limited circumstances where they may share information

¹⁷ Cal. Bus. & Prof. Code §§ 22575-22579.

¹⁸ Toyota Connected Vehicle Services Privacy and Protection Web Portal, <https://www.toyota.com/privacyvts/>.

¹⁹ The FTC has also framed consumer notice as a matter of design and technical innovation. See Opening Remarks of FTC Chairwoman Edith Ramirez at the International Consumer Electronics Show (Jan. 6, 2015), https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf (stating “I am confident that the same ingenuity, design acumen, and technical know-how that is bringing us the IoT can also provide innovative ways to give consumers easy-to-understand choices”).

with government authorities.”²⁰ However, the current state of privacy policies reflects a heavy reliance on general statements of sharing in response to a government request, court order, or as otherwise required by law. OEMs, like many industries, require consumers to blankly trust that their data will be shared with the government in a lawful manner. However, consumers may not expect, for example, their audio and location data to be susceptible to government requests for information, or be aware that they have limited recourse when they consent to services that rely on driver tracking to work effectively.²¹

OEMs have the opportunity to proactively build consumer trust by embracing transparency principles and releasing regular reports on government requests for user data. Transparency reports will help ameliorate the concerns of consumers who “are aware that that they’re under surveillance . . . and are deeply anxious about how their personal information may be used.”²² In an ecosystem where customer data is a competitive advantage, gaining consumers’ confidence is essential, and OEMs would benefit from demonstrating transparent and responsible data stewardship.²³

Connected vehicles offer new and exciting features that, despite their complexities, promise key advancements in safety and convenience. Recent regulatory and legislative activity should provide an impetus to deliver these benefits while also identifying and addressing privacy and security risks. CDT supports the FTC and NHTSA’s efforts to continue engaging OEMs, the wider automotive industry, and related stakeholders to discuss these issues.

More information must be put into the hands of drivers. Existing frameworks may be used to facilitate this. CDT encourages OEMs to review their Privacy Principles to assess shortcomings in industry notice and transparency efforts. Information disclosures are only useful to the extent that consumers, and drivers, are able to access and understand what is happening with their data. Regulators and industry stakeholders should explore how to ensure meaningful consumer access to these sorts of privacy disclosures.

Sincerely,

Joseph Jerome
Policy Counsel
Center for Democracy & Technology

Cassidy Kim
Legal Intern, Privacy & Data Project
Center for Democracy & Technology

²⁰ Automotive Privacy, *supra* at 6.

²¹ See Thomas Fox-Brewster, *Cartapping: How Feds Have Spied On Connected Cars For 15 Years*, Forbes (Jan. 15, 2017), <https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/#34fe6a1a2ef8>.

²² See Timothy Morey, et al., *Customer Data: Designing for Transparency and Trust*, Harvard Business Review (May 2015), <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>.

²³ See *id.*

Appendix A

| Application | Package ID | Analysis Date |
|--------------------------------|----------------------------------|------------------------|
| BMW Connected | de.bmw.connected.na | 7/20/2017, 10:16:55 AM |
| BMW Roadside | com.allstate.bmw | 7/20/2017, 10:16:55 AM |
| Chrysler for Owners | com.chrysler.companion | 7/20/2017, 10:16:55 AM |
| Ferrari Roadside Assistance | com.allstate.ferrari | 7/20/2017, 10:16:55 AM |
| FordPass - Park, Drive, Guides | com.ford.fordpass | 7/20/2017, 10:16:55 AM |
| Ford Remote Access | com.ford.remoteaccess | 7/20/2017, 10:16:55 AM |
| Genesis Intelligent Assistant | com.stationdm.genesis | 7/20/2017, 10:16:55 AM |
| GMC Owner Resources | com.gm.GMCOwnerResources | 7/20/2017, 10:16:55 AM |
| Honda CabinControl | com.honda.cv.cabincontrol | 7/20/2017, 10:16:55 AM |
| HondaLink | com.honda.hondalink.connect | 7/20/2017, 10:16:55 AM |
| HondaLink EV | com.honda.hondalink.ev | 7/20/2017, 10:16:55 AM |
| KIA AR Owner's Manual | com.Tekville.KiaARManual | 7/20/2017, 10:16:55 AM |
| Mazda Mobile Start | com.mazda.mms | 7/20/2017, 10:16:55 AM |
| Mercedes me (USA) | com.mbusa.mercedesme.android | 7/20/2017, 10:16:55 AM |
| myChevrolet | com.gm.chevrolet.nomad.ownership | 7/20/2017, 10:16:55 AM |
| MyFord Mobile | com.ford.mfm | 7/20/2017, 10:16:55 AM |

| | | |
|--------------------------------|--|------------------------|
| myGMC | com.gm.gmc.nomad.ownership | 7/20/2017, 10:16:55 AM |
| MyHyundai with Blue Link | com.stationdm.bluelink | 7/20/2017, 10:16:55 AM |
| MyMazda | com.interrait.mymazda | 7/20/2017, 10:16:55 AM |
| NissanConnect | com.nissan.nissanconnect | 7/20/2017, 10:16:55 AM |
| NissanConnect SM EV | com.aqsmartphone.android.nissan | 7/20/2017, 10:16:55 AM |
| OnStar RemoteLink | com.gm.onstar.mobile.mylink | 7/20/2017, 10:16:55 AM |
| Porsche Track Precision | com.porsche.track.precision | 7/20/2017, 10:16:55 AM |
| Smartphone Link Display Audio | com.mmc.Smartphone_Link_Display_Audio_Manual | 7/20/2017, 10:16:55 AM |
| SUBARU STARLINK | com.subaru.global.infotainment.gen2 | 7/20/2017, 10:16:55 AM |
| Toyota Entune [®] | com.tweddle.toyota.entune | 7/20/2017, 10:16:55 AM |
| Toyota Owners | com.toyota.towners | 7/20/2017, 10:16:55 AM |
| Uconnect [®] Access | com.chrysler.UconnectAccess | 7/20/2017, 10:16:55 AM |
| UVO eco | com.myuvo.evservices | 7/20/2017, 10:16:55 AM |
| Volvo Cars Media Server | com.volvocars.mediaserver | 7/20/2017, 10:16:55 AM |
| Volvo On Call | se.volvo.vcc | 7/20/2017, 10:16:55 AM |
| VW Car-Net Security & Service | com.verizontelematics.vwcarnet | 7/20/2017, 10:16:55 AM |

Given the tendency of OEMs to introduce new connected car apps (instead of updating or replacing previous iterations), we included for analysis only those mobile apps that have been updated within the past year, as of June 20, 2017. The sole exception is Nissan's NissanConnect app, which was last updated in November 2015 but is shown to be in current use per the company's website.