

Introduction

This product is intended to inform decision makers in both the public and private sector on the risks and implications of new and emerging vehicle technology. We stand in the precipice of a new era of vehicle technology, including connected cars, and autonomous and semi-autonomous vehicles which will change the way we live and work. Some early reports predict up to 380 million connected cars will be on the road by 2021. In order to ensure that government and private sector partners can prepare for this new technology, we have outlined several key risks below and have provided recommendations and considerations to address each.

Specifically, our team addressed several issues including the implications of **personally identifiable information (PII)** becoming embedded into our vehicles. The potential for loss of personal data through cyber intrusion will mean yet another vulnerability in our day-to-day lives. We also investigated the near term likelihood that **long-haul trucking and transportation of goods** will likely move to utilizing driverless technology. What will be the likely effects of autonomous trucking on society? We also explored the potential kinetic threats that may come from the use of a **vehicle as a weapon**, either to attack pedestrians, or augmented through the use of explosives. Finally, we note that **regulation** will be an obvious challenge and one that our legislators at the state and federal levels will need to begin thinking about how to address this new technology.

While, this is not intended to be a thorough analysis of these emerging technologies and their associated risks, it is designed to spur discussion at all levels within the US Federal Government and private sector. The sooner discussions begin about the implications of these emerging technologies, the better.

Privacy and Automobiles

A BI Intelligence report¹ on connected cars predicts that over 380 million connected cars will be on the road by 2021. With all of these connected cars comes a lot of connected car data. Fortune magazine predicts that by 2020, autonomous vehicles (AV) will generate about 4,000 gigabytes of data a day.²

As new connected car technology advances, car manufacturers will have greater monetary incentives to process the data, greatly affecting the privacy of the owner's Personal Identifiable Information (PII). Also, many car companies operate on a global scale, so it is also likely that international privacy regulations, such as the EU GDPR may apply.³

¹ <http://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3>

² <http://www.trustarc.com/blog/2017/05/16/privacy-issues-connected-cars/>

³ <http://www.trustarc.com/blog/2017/01/27/connected-car-privacy-guide/>

Data Collection Types

The common types of data currently collected are:⁴

- Event Data Recorders
- On-Board Diagnostic Information
- Location Information – The location of your vehicle and your destination may be collected by your navigation and related systems in order to route you to our destination.
- External Information – Modern vehicles may contain cameras and sensors that are used to gather information about your car's immediate surroundings.
- In-Cabin Information – Many of today's vehicles also contain sensors in the vehicle cabin. Microphones, cameras, and other devices may record information about vehicle occupants.
- User Recognition – Some systems recognize users by physical characteristics such as a fingerprint or face, and therefore may have physical, or biometric, information about users.
- Apps – The vehicle may include interfaces with third-party systems like Apple CarPlay, Android Auto, or other services. Your vehicle may also allow an interface between the applications on your phone and your vehicle.

Privacy Principles

Taking advantage of these new technologies does not mean that consumers must necessarily give up their rights to data privacy. The Automotive Privacy Principles, which guide privacy practices in the automotive industry, went into effect beginning with model year 2017 vehicles. Most major automakers have promised to abide by three main commitments of the Principles:⁵

1. Transparency – manufacturers will provide you with clear and concise privacy policies.
2. Affirmative Consent For Sensitive Data – your consent is required before certain sensitive information is used for marketing or shared with unaffiliated third parties for their own use. This includes three types of data: (1) "Geolocation" (where you are); (2) "Biometric" (physical or health information about you or your passengers), and (3) Driver behavior data.
3. Limited sharing with government and law enforcement – automakers will clearly state the limited circumstances where they may share your information with government authorities and law enforcement.

The Digital Standard

In addition to the Automotive Privacy Principles, the new Digital Standard⁶ outlines a roadmap for helping consumers determine if the organization that obtains your data

⁴ <https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf>

⁵ <https://autoalliance.org/connected-cars/automotive-privacy-2/>

⁶ <https://www.thedigitalstandard.org/>

employs good governance in its use. A subset of this Digital Standard can be applied to automobile PII⁷:

Data collection	Disclosure of the type of user information collected
	Disclosure of how user information is collected
Minimal data collection	The user information collected is only that which is directly relevant and necessary for the service
	Product still works when all permissions not relevant to product's functionality are declined
Privacy by default	Targeted advertising is off by default
	Transmission of user communications is encrypted by default
	End-to-end encryption is enabled by default
	User interface settings which are optimal for privacy are set by default
Data use	Disclosure of what user information is shared
	Disclosure of the types of third parties with which user information is shared
	Disclosure whether user information could be shared with government or legal authorities
	Third party domains contacted by the product are named in the privacy policy
Data control	Users can control the collection of their information
	Users can delete their information
	Users can control how their information is used to target advertising
	Clear explanation of how users can control whether their information is used for targeted advertising
	Users can obtain a copy of their information
	Disclosure of what user information users can obtain
	Users can obtain their information in a structured data format
	Users can obtain all public-facing and private user information the company hold about them
	Privacy controls exist and are effective
Data retention and deletion	All user information is deleted after users terminate their account or remove service from a device
	Disclosure of timeframe in which user information is deleted after users terminate their account
	Disclosure of how long each type of user information is retained

⁷ Adapted from: <https://www.thedigitalstandard.org/the-standard>

Terms of Service and Privacy Policy documents	The Terms of service (ToS) are easy to find
	The ToS are available in the language(s) most commonly spoken by the company's users
	The ToS are presented in an understandable manner
	The privacy policies are easy to find
	The privacy policies are available in the languages(s) most commonly spoken by the company's users
	The privacy policies are presented in an understandable manner
ToS & Privacy Policy change notification	Commitment to notify users about changes to the terms of service
	Disclosure of how users will be directly notified of changes to the terms of service
	Disclosure of timeframe for notification prior to changes to the terms of service coming into effect
	Maintains a public archive or change log of the terms of service
	Commitment to notify users about change to the privacy policy
	Disclosure of how users will be directly notified of changes to the privacy policy
	Disclosure of timeframe for notification prior to changes to the privacy policy coming into effect
	Maintains a public archive or change log of the privacy policy
3rd party requests for user data	The company explains its process for responding to non-judicial government requests
	The company explains its process for responding to court orders
	The company explains its process for responding to requests from foreign jurisdictions
	The company explains its process for responding to requests made by private parties
	The company's explanations include the legal basis under which it may comply
	The company commits to carry out due diligence on requests before deciding how to respond and to push back on unlawful requests
	The company provides guidance or examples of implementation of its process
Transparency reporting	The company lists the number of requests it receives by country
	The company lists the number of requests it receives for stored user information and for real-time communications access
	The company lists the number of accounts affected

	The company lists whether a demand sought communications content or non-content or both
	The company identifies the specific legal authority or type of legal process through which law enforcement and national security demands are made
	The company includes requests that come from court orders
	The company list the number of requests it receives from private parties
	The company lists the number of requests it complied with, broken down by category of demand
	The company lists what types of government requests it is prohibited by law from disclosing
	The company reports this data at least once per year.
	The data reported by the company can be exported as a structured data file
User notification about third-party requests for user information	The company notifies users when government entities (including courts or other judicial bodies) request their user information
	The company notifies users when private parties request their user information
	The company clearly discloses situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users

Table 1. Subset of the Digital Standard

Residual PII

The FBF Consumer Guide also contains a helpful checklist of steps you can take to protect your privacy when selling or renting a car, which includes advice such as:⁸⁹

- Delete your phone contact/address book
- Uninstall and delete any mobile applications in the car
- Delete the data on the vehicle's hard drive storage
- Delete home, work, and favorite places on navigation
- Reset garage door programming

Commercial Vehicles to Pioneer Autonomy

The trucking industry in the United States is critical for the day-to-day operations of thousands of companies, deliver large volumes of products we rely on, and is a vital component of the country's economy. Transportation and logistics made up about eight

⁸ <https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf>

⁹ <https://www.consumerreports.org/privacy/privacy-threat-in-your-used-car/>

percent of US gross domestic product (GDP) in 2016, and the US economic output, in turn, contributed about 15.5 percent to global GDP. That same year, the US trucking industry gained USD 676.2 billion in revenue and transported 10.4 billion tons of freight.

While autonomous vehicle technology may lead many to picture themselves lazily reading in the back seat as their vehicles drive them to and from the office, there are compelling reasons to believe that commercial vehicles—including semi-trucks and many others—will be early adopters of AV technology. AV technology for commercial vehicles can more easily be tested than passenger vehicles, as many companies could test it in closed settings, such as airports, logistics hubs, and industrial farms. Additionally, many semi-trucks run routes predominantly on highways, which offer the advantage of having fewer variables than a passenger vehicle that traverses diverse environments, from garages and parking lots to urban streets to highways.

Importantly, fleet owners have powerful incentives to adopt AV technology. Removing the human driver will reduce labor costs, crashes and damaged goods, delays, and average delivery times, among others. This section explores just a handful of the many implications and questions raised by the adoption of AV in the commercial vehicle space. This technology will undoubtedly cause some painful disruptions, business opportunities, and both advantages and challenges for the US economy and national security. This chapter ends with multiple brief forward-looking recommendations for both government and the private sector as both consider AV adoption.

Current Status

As demonstrated by an April 2017 public listening session hosted by the Federal Motor Carrier Safety Administration (FMCSA), a regulatory body considering regulatory guidelines for commercial vehicle AV technology, the federal government is currently engaged in discussions with the private sector regarding issues such as labor considerations, classification of AV levels, vehicle safety and maintenance considerations, cyber defense, and more.¹⁰ Stakeholders involved include industry organizations such as the Commercial Vehicle Safety Alliance, technology firms such as Alphabet, and commercial vehicle OEMs, such as Volvo Trucks and Daimler Trucks North America.

Autonomous technology is currently being tested on closed tracks and on public highways. In October 2016 Uber delivered a shipment of beer 125 miles in a Volvo semi-truck named Otto. Google's AV company Waymo is currently testing semi-trucks on Arizona highways and on the company's private track. Tesla personnel met with road safety officials in California and Nevada in August 2017 to discuss the possibility of testing autonomous commercial vehicles in those states. While more and more cities and states are permitting the testing of AV technology, commercial vehicles may face an initial disadvantage vis-à-vis passenger vehicles. California, for instance, prohibits testing vehicles weighing over 10,000 pounds, suggesting that the potential damage caused by a commercial vehicle road accident may deter states from permitting AV testing in the short term.

Implications and Risks

10

<http://fleetowner.com/regulations/road-driverless-trucks-clogged-unanswered-questions>.

Disruptive Technology Leads to Rapid Unemployment

One of the largest risks associated with the adoption of AV technology by the trucking industry is the resultant loss of jobs by truck drivers and those who support their operations. According to the US Department of Labor's Bureau of Labor Statistics, in 2014 truck drivers numbered nearly 1.8 million,¹¹ or about 0.56 percent of the US population. Massive layoffs of truck drivers would also result in notable financial strain for their immediate families and reduced inputs into their local economies. The bureau also indicates that the majority of truck drivers only have a high school degree and limited post-high school education, suggesting that their prospects for finding employment are limited in a labor market that increasingly requires a post-secondary degree.

The impact of layoffs and prospects for truck drivers to find new careers will largely depend on the rate of AV adoption in the industry. Naturally, a slower adoption of the technology will likely improve the probability that former truck drivers would be able to find new jobs than if a rapid adoption of AV results in massive layoffs over a relatively short period of time. Numerous studies have found a positive correlation between rising unemployment and rising crime rates in the United States, suggesting that those communities hit hardest by truck driver layoffs may begin to experience increases in crime, which could compound their economic disadvantage by dissuading local investment.

A mitigating factor to this threat is that there are very real concerns about purely autonomous vehicles. As described below, there are law enforcement, insurance and pure public safety concerns associated with setting trucks loose on America's roads without a human on board. It may well prove that legislatively a hybrid model is what will work, where companies get the benefits of improved logistics efficiencies and human drivers get less onerous workloads.

Businesses and Government to Gain Efficiencies

The adoption of properly developed AV technologies into commercial vehicles is likely to offer revenue gains and cost savings for the entities that own the vehicles and for their clients. Organizations that operate large fleets of semi-trucks, such as major retailers, manufacturers, and logistics companies, will reduce costs associated with driver wages and benefits, vehicular accidents, fuel consumption (due to more efficient driving), and faster delivery times (trucks will no longer have to stop for the driver to sleep). Organizations that manage facilities with large numbers of commercial vehicles, such as airports, logistics hubs, and ports, will benefit from similar changes as well as efficiencies from reduced gaps between functions involving vehicles. For instance, a large port could leverage AV, V2V and V2I technologies to ensure that a container vessel, cranes, semi-trucks, and a mobile x-ray unit can all communicate and coordinate their operations within fractions of a second that would otherwise present a high risk if these vehicles were manned.

Public Safety Risks

Autonomous vehicles are not as close to reality as many of their Silicon Valley boosters would like us to believe. For example, an official at the New Mexico Department of Motor

¹¹ <https://www.bls.gov/ooh/transportation-and-material-moving/heavy-and-tractor-trailer-truck-drivers.htm>.

Vehicles presented in Detroit about a recent test done between two trucks: one fully autonomous and one with a human driver.

During the test, conducted at a remote desert location, the “surprise event” was a front tire blowout. The human driver with more than a decade of experience, immediately responded by slowing the truck, checking for environmental traffic, and eased the truck off to the side of the road. The AV truck just kept going, trying to fulfill its mission of delivering to its destination.

When addressing concerns of public safety, questions arise around accident liability. Who is responsible when an AV fails to distinguish a pedestrian in its path or a white truck against a white background and a crash or fatality ensues? The car manufacturer, a component supplier or the owner of the AV? What if environmental conditions impacted the crash? What about the cases of hybrid vehicles where ideally human input overrides AV error? Such unknowns change the architecture of liability and require more research, feedback and insight.

Criminality and Law Enforcement

One of the biggest problems with fully autonomous vehicles is that law enforcement and customs officials fear the technology may cause a spike in criminal activity. Currently, in order to smuggle people or narcotics cross-border or domestically, at least one person (i.e. the driver) has to put him or herself at risk of incarceration. Occasional media reports of semi-trucks seized with narcotics or human cargo indicate that criminals can still find willing or persuadable drivers. But, drug cartels and human traffickers would likely embrace autonomous commercial vehicles, because the only risk of loss to them is the capital loss of the truck and cargo. AV technology would largely remove the human factor from the equation once fleets have replaced human drivers with AV trucks. Unless fleets implement measures to prevent criminals from intercepting or tampering with their vehicles, authorities should expect a spike in such activity the moment drivers are removed from the cab.

Similarly, while suicide truck bombers are clearly found for terrorist purposes, there have been few instances of that in the United States so far. But if trucks or cars become fully autonomous, this will increase the opportunities for terrorists to launch vehicle-borne improvised explosive device (VBIED) attacks.

These public safety fears will likely be stoked by the Teamsters Union and other organized labor groups, who will bray loudly about the unacceptable risks to public safety by having robots drive trucks across our country and – gasp! – through our cities, *near our schools!*

Regulatory Patchwork Could Hinder Adoption

A diverse array of federal, state, and local regulations and standards on autonomous commercial vehicles would likely disrupt or limit the technology’s adoption. However, proponents of autonomy should view current federal legislative activity positively. In July 2017, the House Energy and Commerce Committee passed a draft bill that would largely empower the federal government to regulate the technology’s testing and implementation. The full House has yet to vote on the bill. The Senate is expected to vote on a similar bill in the autumn that is likely to also grant the federal government broader powers to regulate autonomy. Maintaining this momentum will be important to avoid the costs and complexity that would come with a diverse array of local regulations.

Supply Chains to Face New Cyber Threats

For all its inefficiencies, the human factor has so far kept cyber threats from posing an insurmountable threat to supply chains. As companies and governments begin to increasingly rely on self-driving vehicles to meet the needs of transferring products across the country and the world, their operations will become increasingly vulnerable to cyber security disruptions. Imagine that the country's largest meat producers (e.g. Tyson Foods, Inc., Smithfield Foods, Inc., JBS S.A.) have all transitioned to fully autonomous fleets. A cyber intrusion into one or more of these companies that causes all vehicles to stop—or even deactivates the onboard cooling systems—would not only delay shipments and hit profit margins, but would also threaten US food security as countless quantities of meat spoils and undermines certainty in the ability of producers to get their product to market.

Recommendations and Considerations Moving Forward

- The private sector and government intelligence and law enforcement authorities may need to find improved and more nimble ways to interact and share intelligence to minimize opportunities for organized crime and hackers to exploit autonomous commercial vehicles. Recent forums that have brought stakeholders together to explore these issues, such as the National Motor Freight Traffic Association, Inc. meeting and the United States Embedded Security for Cars Conference in June 2017, are positive steps forward, but stakeholders will need to formalize procedures and relationships for intelligence sharing and incident response.
- Stakeholders and lawmakers concerned about developing regulations on autonomous vehicle technology should begin to understand the full impact that this technology will have, and the harmful impact that varying regulations across state lines may place on the technology's development and the US' leadership in the industry. AV technology development firms, OEMs, logistics firm, and others should jointly articulate AV's positive impact for US businesses and its safety record as testing and adoption progress.
- Companies that anticipate layoffs of truck drivers and similar personnel should begin to work with lawmakers early to develop strategies for supporting the unemployed while minimizing disruptions to business operations or the adoption of AV technology.
- Alternatively, companies should be prepared to change how drivers are tasked, and prepare for new laws allowing, for example, longer continuous driving periods per day coupled with more flexible rules around humans. For example, truck drivers could become like bus drivers – working in shifts across routes, permitting greater drive-time efficiencies while enhancing public safety.
- Executives of companies with complex or large supply chains or with large fleets must come to appreciate that as their firms adopt AV and other technologies that streamline their operations and reduce costs, their firms will likely grow more vulnerable to cyber attacks and will need to make earnest investments in IT security hardware and skilled personnel to mitigate the growing risk.

- The US federal government will need to consider how to forge enabling regulations and traffic laws to permit AV commercial vehicles to cross international borders. Developing mutual recognition or universal standards between the United States, Canada, and Mexico should be an early priority for each of these governments to shore up legal and commercial certainty for a North America that is increasingly interconnected with complex supply chains.

Use of Vehicles as a Weapon

The emerging era of connected and autonomous cars affords us new efficiencies and freedoms not realized in previous generations. However, as this paper has outlined, there are also risks; in particular the potential exists for nefarious actors to use a vehicle as a weapon. Regardless of ideology or purpose, we have seen the unfortunate result of violent extremists who were able to kill and injure simply by using a vehicle to ram pedestrians.

- In July 2016, an attacker drove a 19-ton truck through a crowd of people celebrating Bastille Day in Nice, France.
- In March 2017, an attacker killed four pedestrians on the south side of Westminster Bridge in London, before exiting the vehicle and attacking others with a knife.
- Just three months later, multiple attackers in a rented van mounted the curb along the tourist-heavy London Bridge killing three. They too exited the vehicle and continued the killing with long knives. Weeks later another attacker drove a van into pedestrians in Finsbury Park, London injuring eight.

These recent events highlight the obvious dangers of a vehicle of any size being used as a weapon; however, if you add in the use of improvised explosive devices, the potential casualties increase exponentially. From the Bath Township massacre in 1927—which is known as one of the first car bombs—to modern incidents such as the tragedy in Oklahoma City, numerous incidents across history have illustrated the potential for death and destruction when bad actors use vehicle-borne improvised explosives devices (VBIED).

The success of a VBIED attack is often determined by whether or not the vehicle is able to be positioned close to the target. Protective measures such as bollards, checkpoints, and other elements have been placed to protect critical infrastructure around the world. Suicide attacks have often bypassed some level of security with drivers ramming or attempting to drive around security features. Finding a committed member of a terrorist or criminal plot to conduct such an operation is challenging. However, if there is no need for a driver, the potential risk increases.

Imagine a scenario where an autonomous vehicle is loaded with explosive material and sent on its way towards a specific target. The potential to target VIPs en route, or to simply direct a vehicle to drive to a specific location and park would be very plausible.

Many critical infrastructure facilities will have to “engage” with driverless vehicles arriving to pick up people within their protected zone. Policies with regard to vehicle search may need to be modified for driverless scenarios where vehicles enter and exit through their gates each day. Discussions with manufacturers about how to ensure that an

autonomous vehicle, arriving to pick up someone at a guarded facility, will stop at the appropriate spot, for the appropriate amount of time to be searched, will be critical.

Beyond that, current vehicle search procedures should be adequate to detect the presence of explosive material, and current protection measures to keep vehicles from entering restricted areas should be effective against an autonomous vehicle intended to be a bomb.

Regulatory Practices in the Automotive Industry

Current regulatory practices on Highly Autonomous Vehicles (HAV) by National Highway Transportation Safety Authority (NHTSA) should be implemented by the autonomous vehicle industry in order to achieve standardization. Despite the NHTSA not having the authority to pre-approve new motor vehicles or new motor vehicle technologies, the agency suggests that any introduction of technologies to vehicles should meet the existing Federal Motor Vehicle Safety Standards. This assessment is made based on specific suggestions noted by NHTSA's September 2016 Federal Automated Vehicle Policy.

- NHTSA has four primary “tools” that the Agency uses to address the introduction of new technologies and new approaches to existing technologies, which are: 1. Letters of interpretation 2. Exemptions from existing standards 3. Rulemakings to amend existing standards or create new standards and 4. Enforcement authority to address defects that pose an unreasonable risk to safety.
- A vehicle or equipment manufacturer need ask NHTSA about a new technology or vehicle design only when it will not comply with applicable standards, or when there might be a question as to compliance.
- Vehicles that have been granted exemptions and are intended for sale must have permanent labels affixed to their windshield or side window that list the standards (by number and title) for which an exemption has been granted, along with the exemption number from NHTSA. 49 U.S.C. § 30113(h); 49 CFR § 555.9; FAST Act, Sec. 24405.

Regulatory Practices in Other Autonomous Transportation Devices

Although the automotive industry is now faced with many challenges of implementing autonomous technology, the airline industry had the “autopilot” technology implemented in their airplanes. NHTSA notes that there is a need to focus on the Federal Aviation Administration (FAA) because its challenges seem closest to those that NHTSA faces in dealing with HAVs. FAA uses an agency pre-market approval process to regulate the safety of complex, software-driven products like autopilot systems on commercial aircraft.

- There are five phases for FAA's “type certification” process for approving aircraft design that move from early project concept and initiation through post certification activities. All phases contribute to improving safety and serve to mitigate cost and project risk.

- The FAA is responsible for overseeing the expert designees work and determining whether designs meet FAA requirements for safety.

Conclusion

There is no question that autonomous vehicles will offer many benefits to our world, from saving us time to increasing mobility. However, numerous risks already exist and will likely be amplified over time as new technology evolves. Vehicles have already begun to become part of a broadening world of connected systems. The risk of losing personally identifiable information through cyber intrusion will be part of the risk equation for those who adopt the technology. Early use will likely revolve around the transportation of goods through the trucking industry. In the relative near-term, fully autonomous vehicles will likely put millions of truck drivers out of work. Nefarious actors will likely attempt to utilize the technology to advance the impact of kinetic attacks, such as using an autonomous vehicle to ram pedestrians, or enhancing the attack with explosives to build a driverless VBIED. Finally, there will be significant legal and regulatory hurdles involving accident liability and new vehicle technology standards that will need to be addressed in the future. Government and private sector decision makers should immediately begin addressing these risks in order to mitigate them within their organization.

Additional Reading

<https://epic.org/privacy/edrs/>

[automobiles.com/privacy-policy/](https://www.automobiles.com/privacy-policy/)

<https://www.nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html>

<https://www.pcmag.com/article2/0,2817,2429806,00.asp>

<https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected>

<http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2728&context=lawreview>

<http://blog.legalsolutions.thomsonreuters.com/law-and-techology/smart-cars-privacy-and-security/>

<https://www.ftc.gov/news-events/press-releases/2015/10/ftc-testifies-proposed-legislation-addressing-privacy-security>

<https://www.forbes.com/sites/amadoudiallo/2013/12/16/connected-car-data-privacy/#6f3a39d143db>

<https://www.iamthecavalry.org/domains/automotive/5star/>

<https://www.consumerreports.org/privacy/privacy-threat-in-your-used-car/>

<https://www.edmunds.com/car-technology/car-technology-and-privacy.html>

<https://iapp.org/news/a/connected-cars-security-and-privacy-risks-on-wheels/>

<https://www.law360.com/articles/650332/connected-cars-a-global-privacy-challenge>

<https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf>

<https://github.com/TheDigitalStandard/TheDigitalStandard>