




Your connected car is talking. Who's listening?

**Moving the data-driven user
experience forward with value,
security and privacy**

@YourCar: Feeling extra #chatty today.





@YourCar:
"Monday. 8:23 a.m.
37 degrees. Pulling out
of the driveway with
Passenger Alex and
heading to the office
at 123 Main Street."

Contents

	About the authors	1
	A message from Gary Silberg	3
	Securing the high value of data	5
	Big data speaks volumes	8
	The risky road ahead	14
	A closer look under the hood	19
	Cybersecurity in a connected car	22
	Reaching your data destination	24
	About KPMG	28



About the authors



Gary Silberg is KPMG LLP's (KPMG) national sector lead partner for the automotive industry. With more than 25 years of business experience, including more than 15 years in the automotive industry, he is a leading voice in the media on global trends in the automotive industry. He advises numerous domestic and multinational companies in areas of strategy, mergers, acquisitions, divestitures, and joint ventures. For the past 5 years, he has focused on the intersection of technology and the automotive industry with groundbreaking research on self-driving cars, connectivity, and mobility-on-demand services.



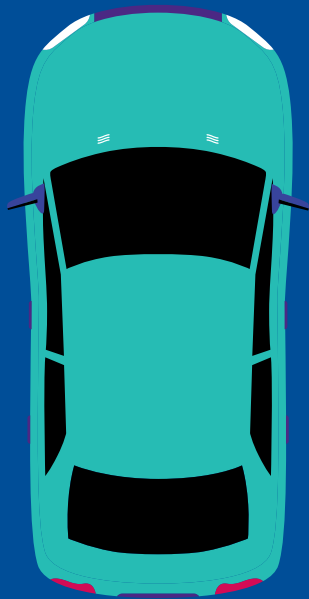
Ron Plesco is a principal and the national lead of the KPMG Cyber Investigations practice. He and his team focus on cyber threat intelligence and cyber breach investigations. He is an internationally known information security and privacy attorney with 18 years of experience in cyber investigations, information security, privacy, identity management, computer crime, emerging cyber threats, and technology solutions. Concentrating on the automotive industry, he regularly presents on vehicle hacking and the cybersecurity concerns regarding interconnected vehicles. Prior to joining KPMG, he was chief executive officer of the National Cyber-Forensics and Training Alliance, where he managed the development of intelligence that led to more than 400 worldwide cyber crime arrests in 4 years and prevented more than \$2 billion in fraud.



Doron Rotman is a managing director in KPMG's Advisory practice. He is the national privacy service leader, a member of KPMG's national Privacy Leadership Council, and a member of the KPMG International Privacy Leadership team. With more than 28 years of experience, he is focused on providing privacy, security, and information governance services to large organizations. He has extensive information technology audit, accounting, and finance experience, as well as extensive knowledge of the high-technology, financial services, healthcare, manufacturing, utilities, and government industries.



Danny Le is a principal in KPMG's Advisory practice with a specialization in cybersecurity. He spent the last 10 years building KPMG China's consulting business, most recently serving as the head of KPMG China's Automotive practice and a member of KPMG's Global Automotive Steering Committee. He brings specific experience in helping automotive companies develop and implement mobility services and move traditional business processes online. He is also one of the founding partners of KPMG's Information Protection and Business Resilience practice in the United States, where he leads numerous global accounts.







A message from Gary Silberg

Today's vehicles are more "wired" than ever before – offering connectivity similar to what we expect at home, in our offices and on our mobile devices. And that connectivity is absolutely awesome for drivers and consumers. However, it does come with some inherent risks.

In our cars, which have basically evolved into computers on wheels, we are surrounded by data, software and sensors. And the technology is advancing by the minute. Very soon, our cars will become the center of our connected lives – whether helping us avoid those horrendous traffic jams, entertaining us on the go, detecting problems with our cars before they become massive repair jobs, or most importantly keeping our families safe and helping us avoid unnecessary and tragic accidents.

Onboard software and devices now capture how you drive, where you go, who you call, what you listen to, and which personal devices you're connecting to. Unfortunately, all of this data and connectivity, despite being on a moving vehicle, provides a target for would-be hackers.

Unlike your phone or your bank account, a simple reboot or software update isn't doable in a moving car. Your car isn't like your other devices. A vehicle breach can be life-threatening - especially if the vehicle is driving at highway speeds and a hacker gains control of it. Can you imagine the potential consequences of someone other than you controlling your vehicle?

So what does all of this mean for automakers going forward?

In this paper, we explore these two worlds – the one in which data means fantastic value, and the one in which data means risk. We'll show you how to balance the two, leveraging data insights to offer your customers an unbelievable driving experience while at the same time protecting the data like it was your own.

Getting this right can create tremendous growth opportunities for your company. Getting it wrong can significantly damage your brand.



Gary Silberg
Partner and National Automotive Leader





Securing the high value of data

So you need a new car? If you're like many car buyers today, you're probably not too hung up on horsepower or miles-per-gallon. What matters most to you is your driving experience—how well it integrates with the rest of your life, especially your digital life. In the not-so-distant future, the car will take on another persona—your mobile digital identity. Who will be the first to create the iPhone® on wheels: An integrated vehicle and digital identity?

Today's consumers have become accustomed to ubiquitous, seamless connectivity of all of their personal mobile devices everywhere they go—and their vehicles are an essential part of the equation. The automotive sector is responding to their expectations by manufacturing ever more complex and technology-enabled "connected cars," which can communicate remotely with a vast digital ecosystem of other devices. The master onboard computer system of an average car today has more than 60 wired and wireless connections to draw in data from the external world, including sensors, GPS units, infotainment platforms, and mobile devices. You as a consumer probably don't even consider the fact that your car is talking about what "it" and you are doing.

Today's car companies are masters at mining data to understand their customer base.

To car owners, the value of a connected car is software and electronics that enhance the user experience, making driving easier, safer, more personal, more fun, and more productive. To automakers, the value of a connected car is its data and what it can tell them about their customer and their experience with the product.

Equipped with high-tech software and systems, connected cars collect billions of bits of data about driver habits and preferences and real-time vehicle metrics and diagnostics. This data can unlock powerful insights about customers, such as driver needs, driver behavior, and vehicle performance, which automakers can use to drive smarter decisions and improve vehicle safety. Additionally, automakers can monetize the data with new business models that tap into entirely new sets of customers.

Perhaps, most important, from both the OEM and the customer's perspective, is that the telemetry data inside a connected car's sensors can significantly improve safety. Automotive manufacturers can use it to encourage drivers to stay alert and obey the rules of the road, to predict and prepare for poor driving conditions, to get instant emergency help, or—through driver-assist technologies—to even avoid accidents.

**@Your Car:
"GPS shows
construction on
Third Street. Detouring
to Oak Ave. Texting office
manager at 555-555-9876
that Passenger Alex is
running 2 minutes late."**

We think managing telemetry data in the car to enhance vehicle safety is where OEMs should ultimately focus their data-related efforts, as it is a stronger competitive play than leveraging data to enhance user experience, where many consumer-focused companies from outside the industry are already well-established. There will continue to be a lot of competition to leverage user data to deliver superior customer experience. Although there remain ethical and privacy concerns about whether consumers will be able to opt out of providing their private data to car manufacturers but still realize the benefits of a safe, functioning vehicle, we think leveraging telemetry data to make sure people are absolutely safe in their vehicles is where OEMs can dominate.

As cars become ever more complex computers or endpoints-on-wheels—virtually exploding with data and information—it leads to exciting new opportunities. But it also requires a different way of thinking about risk and brand maintenance.

Automakers can only capitalize on the data if they can ensure it is being used appropriately. Just as the data contained in a connected car's systems has inherent value, it also carries many risks. Data can be hacked, lost, or mishandled, disrupting car users' lives, possibly putting them in physical danger, and leading to serious financial, regulatory, and reputational consequences for the automaker. Quality and integrity of data are also important; data that has been altered cannot be used by the business to generate value. In addition, there may be a conflict between the privacy of individuals and safety considerations.

Automakers invest millions and millions of dollars toward building and maintaining a brand. So just imagine the brand fallout if a car is considered "hackable" or insecure. Or just imagine if a manufacturer becomes known as "that car company that just got hacked."

In business today, including and perhaps *especially* in the automotive industry, data is the new critical asset. That is why we believe **today's automakers must maintain consumer confidence in their brand by becoming data protectors**. Our experience shows those that expertly handle, manage, analyze, and safeguard the valuable data flowing in and out of a connected car will be able to tailor superior experiences that keep car owners satisfied and car buyers interested.

In this paper, we will explore how car manufacturers can differentiate themselves in the market by securing high-value data to enhance the automotive experience and address security and privacy concerns.



"Cars and trucks have evolved into highly complex computers on wheels, with increased connectivity that presents some real and important cybersecurity risks, the most significant of which is safety. Unlike most consumer products, a vehicle breach can be life-threatening, especially if the vehicle is driving at highway speeds and a hacker gains control of the car. That is a very scary but possible scenario."

—Gary Silberg, Partner and National Automotive Leader, KPMG



"The new asset in the automotive business is data. Data is becoming a currency, with actual value, and it must be protected. Security needs to be invested in."

—Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services



Big data speaks volumes

As they enable greater and greater levels of connectivity in their vehicles, the automakers who own the data stream are positioned to capitalize. Because, clearly, the volumes of data in a connected car speak, well, volumes. The question is: What is the data saying?

The most successful automakers will use strategic data curation and predictive analytics to increase customer confidence, comfort, and safety, optimize their own operations, and introduce new ways to generate revenue.

Increase customer confidence, comfort, and safety.

Automakers can use data to curate every aspect of the customer relationship throughout the entire customer life cycle, from awareness to purchase to maintenance and upgrade. Indeed, connected cars are changing the car-buying experience to be more data-driven and therefore more personal and satisfying. Consider your pleasure if you walk in the dealership to meet a dealer who already knows who you are and what you are interested in, and he immediately connects you with the right products, configurations, and add-ons to meet your needs.

Once you own the car, the data in connected vehicles leads automakers to insights into your driving habits, the kinds of roads you take, how many passengers you carry, the type of music you listen to, and much more. Those insights allow automakers to enhance and customize your experience inside the car. For example, imagine the increased satisfaction created by helping a busy mom warm up her car before a wintry school drop-off, an overworked businessperson work more efficiently on the road, an accident victim get emergency assistance, or an excited road-tripper arrive at his destination traffic-free accompanied by the perfect music selection for his mood.

For automakers, the natural play is to use big data from connected car networks to make our roads safer, helping people drive better, avoid real-time hazards, access rapid response services, get enhanced routing and traffic management, and drive more comfortably.

Automakers can also compete for digital user experience, but they will be challenged by formidable players like Apple, Google, Amazon, Spotify, etc. While OEMs can gather the data, they do not yet have the shopping sides to provide buying opportunities or music or entertainment libraries to own the customer. This is a very large market opportunity to explore.

The most successful automakers will use strategic data curation and predictive analytics to:

- 1 Transform the customer experience.**
- 2 Optimize their own operations.**
- 3 Introduce new ways to generate revenue.**

Four key data flows driving the experience

Performance: Connected cars deliver wear-and-tear warnings, maintenance predictions, and maintenance appointment scheduling by collecting status updates on vehicle components like valves and brakes through onboard sensors. This data is shared with the OEM cloud through the telematics unit, enabling automakers to aggregate onboard performance readings from the entire vehicle fleet and obtain unprecedented insights on failure rates and maintenance needs. The data is also shared with the OEM supply chain to predict component demand, with insurance companies to predict which cars break down the most and with dealers and repair shops for preemptive maintenance.

Infotainment: As the in-dash consoles of connected cars collect driver and passenger usage data, the GPS collects location data and the telemetry unit connects users to content, business, and service providers, the cycle creates opportunities for expanded media consumption, targeted advertising, and market research.

Business: Connected cars help drivers connect to the corporate network and do business from the road, using hands-free calling, automated assistants, and navigation services.

Health: Using onboard sensors, connectivity with external devices, such as Fitbits or wearables, and telematics to collect data on vital signs, prescriptions, and medical histories, connected cars offer owners emergency response, medical reminders, and linkages to healthcare providers, lifestyle apps, and health and wellness services.

In our 2014 white paper *Me, My Car, My Life*, we accurately predicted many of the automotive industry changes we would see in the ultraconnected age.¹ Now, our view is OEMs that anticipate the future connectivity of infrastructure, and put sensing devices inside their vehicle fleets that can communicate with them, will be able to offer drivers the ability to know what will happen around a curve or at an intersection—even before their car gets there. They will have much better information to prevent accidents, help cars drive more efficiently, and create comfortable rides. Those are all clear differentiators for OEM brands.

As OEMs look to turn connected car data into insights that improve passenger comfort and safety, they need to strike a balance between protecting user privacy and enhancing their safety. We will explore this issue later in the paper.

Optimizing operations

Automakers can also use the data to optimize the performance, reliability, and safety of individual vehicles or entire fleets. The onboard sensors of connected cars collect status updates on vehicle components like valves and breaks. They enable automakers to track wear and tear and ensure vehicles are road-ready from a mechanical perspective. For example, your tires have low air pressure, your fuel efficiency is deteriorating, or your alignment is off. In the future, telematics could also be used to increase the comfort of driving, leading to better ride quality, smoother traffic, or even better sights or scenery, for example.



“In the future, OEMs may have opportunities to work with companies that own infrastructures, like paint manufacturers responsible for lane markings on roadways and companies that install street signs and stop lights. Parts of the infrastructure across the nation could eventually have embedded RFID, software chips, or other technology inside them which enable cars to “see” the road better.”

—*Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services*

Sensor data allows automakers to predict maintenance needs and even proactively schedule maintenance appointments. The integrated systems in your car even automatically provide you with alerts to product updates and relevant sales promotions, so you will not have to worry about a sudden mechanical problem or about missing out on a great offer. Other services enabled by telematics data include prebooked parking, car wash, or car pickup, service, and delivery.

And when the performance data is aggregated across entire fleets of vehicles, automakers can obtain unprecedented insights on failure rates and maintenance needs. These can be used to predict component demand, address potential recall issues before they get out of hand, and inform future research, design, innovation, and product development efforts.

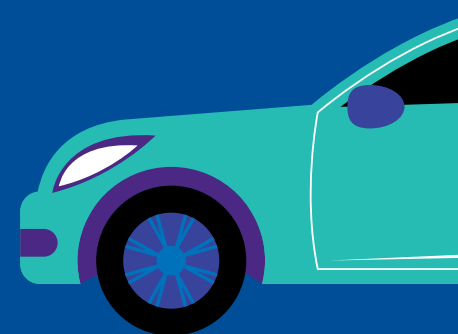
Generating revenue

The most innovative automakers will monetize data to support existing and emerging business models. Many OEMs are launching mobility services offerings, like premium parking, car delivery services, car rental, fuel and charging, car sharing, and concierge services. They are looking to seize a larger portion of the global automotive market by selling products and services around cars, rather than just cars themselves.

But when it comes to other revenue opportunities, OEMs will have to fight. This will be a competitive battle between mobile providers, app makers, connected cars makers, and cloud providers. Look at the investment that Google, Apple, and Microsoft have already made in owning the car infotainment interface.

What’s clear is this: Those who own the data win.

Any data that delivers a detailed customer profile—i.e., John, a white male, age 48, who drives a Honda Civic, lives in San Francisco, primarily listens to Warriors basketball game broadcasts, stops at Starbucks, and



¹ *Me, My Car, My Life* (KPMG, 2014)

Should OEMs get into the content business?

The enigmatic billion-dollar electric car start-up in California, Faraday Future, apparently believes OEMs should get into the content business. There are numerous speculations and discussions about how Faraday Future and LeEco, the Chinese online entertainment firm it is partnering with, intend to converge diversified business models of consumer electronics, media, and entertainment into a subscription-based electric vehicle.

Source: LeEco plans a big electric car factory in China (Fortune, August 11, 2016)

**@YourCar:
"Electric car battery is fading more quickly than expected. Scheduling visit to service center for diagnostics and preventative maintenance on Wednesday during one-hour window on Passenger Alex's calendar."**

spends 2 hours per day in traffic—has huge value to advertisers and market researchers. Coupled with GPS data, location-based advertising through a connected car is an especially powerful opportunity, i.e., when John drives by a highway billboard, an advertiser knows it instantaneously and serves up an ad ("Big sale on Warriors jerseys!") tailored specifically to him.

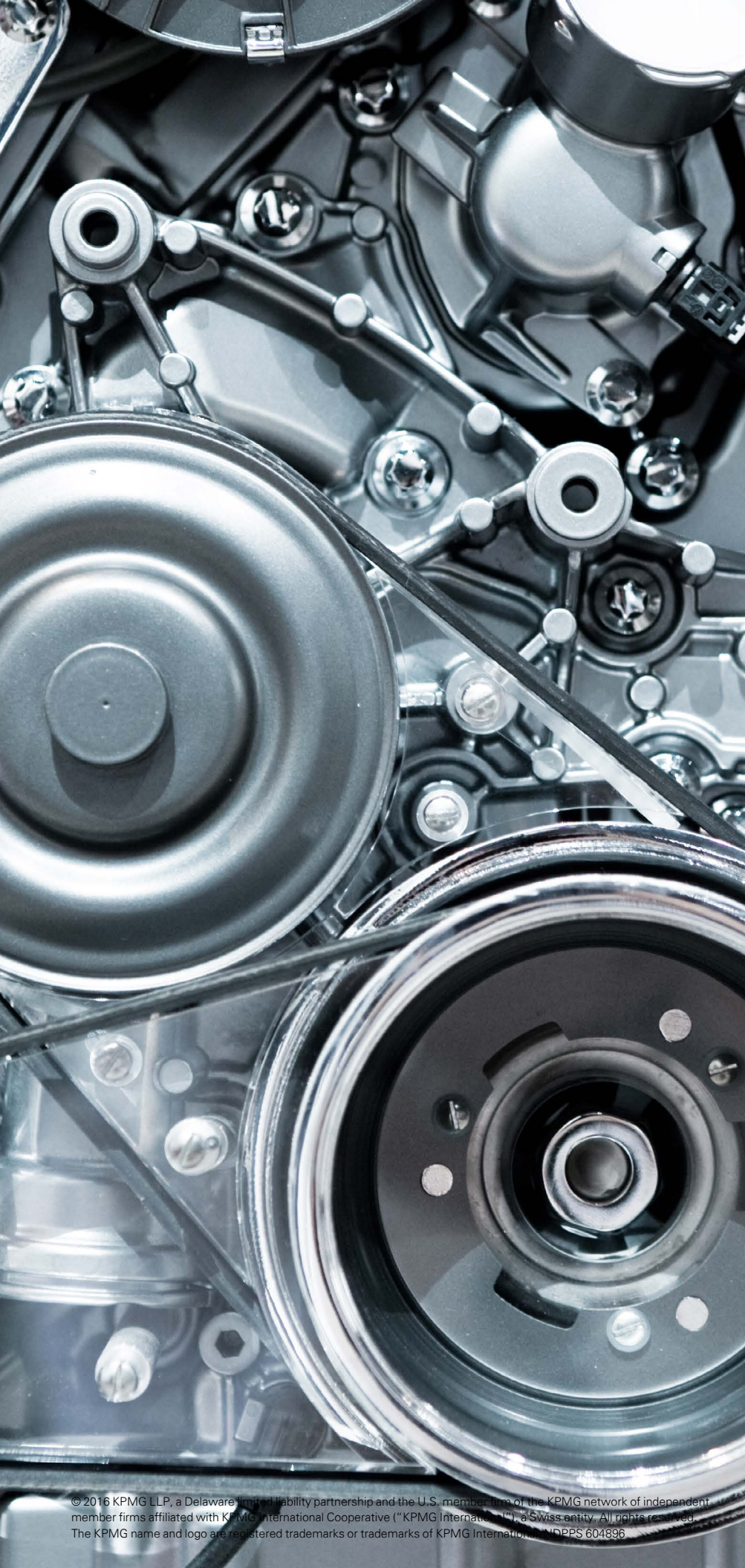
Then, there is the information in a connected car about people's driving behavior, e.g., John likes to go 15 miles per hour above the speed limit and is often navigating traffic-clogged intersections in downtown Los Angeles. While there are currently controversies over whether insurance companies should track users and charge them based on driving behaviors, it is clear insurers are likely to be very interested in that data, as it could potentially help them better tailor premiums.

As car companies evolve and unleash new service-oriented business models, we expect data monetization to be a significant opportunity in the near future. But OEMs should be aware of some potential issues.

For one, data monetization can take the revenue out of the automotive industry and put it elsewhere. For example, cars are free, but electric charges, maps, music, and parking cost money. This could change the dynamics of the business drastically. OEMs that get into the services business could even outsource the manufacturing process.

In addition, the tax implications of where and how that data can be monetized will require automakers to give careful consideration as to the jurisdiction and legal entity that economically benefit from the data.

What's more, sharing personal information presents a huge privacy issue (more on that later in the paper). Given the complexities over data ownership, we have not yet seen automakers reap value by selling their data to advertisers, market researchers, or other third parties.



“Automakers can manage its service business to match the capacity of service centers so that there are less peaks and lulls. They can spread out service visits so they don’t come all at once. This lowers the capital investment required for service centers and increases utilization of the infrastructure assets that OEMs have already invested in.”

—*Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services*



“OEMs can be the broker of data on behalf of drivers. If John drives very conservatively, usually only for small distances, he may want to share that data to see if he can get a lower insurance rate. OEMs with a strong understanding of security and privacy can offer this option, which facilitates a better match of customer to service.”

—*Gary Silberg, Partner and National Automotive Leader, KPMG*



The risky road ahead

Now that we have examined the value of the data, let us look closer at two key categories of risk related to connected car data that deserve the attention of automakers: data security and data privacy.

Data security

A woman drives down a city street while her car reads her work e-mail to her. She pulls over into a parking lot and orders a latte from Starbucks using an e-commerce app. Because her smart phone is synced to her car, her corporate information, work-related communications, and credit card information instantly enter and exit the car's computer. Is that data protected? Who is responsible for protecting it, the woman's employer, using corporate security controls on the phone, or the OEM? The payment app that stores her credit card number?

Data security involves protecting the confidentiality, integrity, and availability of data. Poor data security can result in theft of money, identity, or intellectual property—or much worse.

Connected cars take data security in an entirely new direction, because the stakes are so high. The three tenets of the National Institute of Standards and Technology (NIST) information security framework—confidentiality, integrity, and availability of data—are paramount when human lives are at stake. At worst, a system hack can cause a crash, risking injury or death to car drivers or passengers. What if your car is hacked while you are approaching an intersection or driving 70 miles per hour down a crowded highway? Or, what if a thief hacks your electronic key signature and drives off with your vehicle, a method of vehicle theft that the National Insurance Crime Bureau says is on the rise.²

A cyber attack on a vehicle can take many forms. Hackers can target an individual vehicle's control systems, an automotive manufacturer's corporate systems, or connected systems that contain personal information of drivers and passengers. These attacks are happening: Just search the Internet for car hacking and cyber threats and see what comes up.

While there are not yet reports of real cyber criminals taking control of a moving vehicle, over the last few years, hacker conferences have demonstrated this scenario to be plausible. In July 2015, *Wired* hired two hackers to see if it could be done. Using a laptop computer located 10 miles away, the hackers were able to take command of a reporter's Jeep Cherokee as it sped through downtown St. Louis, adjusting the climate controls, changing the radio station, projecting their own images through the interior

² *Thieves go high tech to steal cars (Wall Street Journal, July 5, 2016)*

Eighty-two percent of consumers would be wary or never buy from an automaker if that brand experienced a car hack.

Source: *Data Loss Barometer* (KPMG, 2016)



"With the Internet of Things, including connected cars, the information security model should also include physical security considerations."

—*Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services*



"Economic risk associated with data security can be significant, such that how a company proactively manages such risk should be factored into an organization's tax planning."

—*Steven Davis, Principal, International Tax, KPMG*



“Data security is about protecting the confidentiality, integrity, and availability of data. In a connected car environment, it’s about ensuring data is limited or restricted to stakeholders that have appropriate permission to see that information.”

—Doron Rotman, Managing Director and Privacy Service Leader, Advisory, KPMG



“Your car is talking. For the car and our data, the question is: ‘Who owns the data and whose responsibility is it to secure it?’ Is it the vehicle manufacturers, the third party who designed the car’s software, the app maker, or the driver’s telecommunications provider? These are risk governance questions the industry still needs to answer.”

—Ron Plesco, Principal and National Lead, KPMG Cyber Investigations

digital display, and even remotely stopping the transmission and brakes.³ After the incident, Chrysler recalled 1.4 million vehicles and upgraded its network to ensure remote hacking could not take place and add in additional security features.⁴ Later, in March 2016, the Federal Bureau of Investigation (FBI) and the National Highway Traffic Safety Administration warned the public against this exact scenario, warning drivers about the threat of over-the-Internet attacks on cars and trucks.^{5, 6} However, in August 2016, the same hired hackers were able to mess with the engine control unit (ECU), work the steering wheel at speed, increase cruise control settings, and activate an electronic parking brake without physical access to the car.

Another type of attack against the car is to steal the vehicle by remotely hacking the doors to gain entry and steal the car. This exploitation has been all over the news during the last two years.

Cyber attackers also target the automotive industry directly. They have breached the procurement and payroll systems of manufacturers and suppliers to steal their intellectual property, merger and acquisition information, employee and customer data, banking data, and more—anything of fungible value on the cyber underground or for wire transfer fraud. They also target the industry to steal consumer information, such as names, birthdates, social security numbers, loan information, and social media information. This targeting takes place against corporate systems, especially e-commerce systems, such as loan/lease payments and service payments.

Finally, individuals are targeted through the interconnected vehicle interface, wherein threat actors attempt to get into the phones or tablets of drivers while they are connected to the car. As vehicle entertainment becomes a more dominant marketing channel, we could even envision a scenario in which disreputable advertisers push rogue junk or pop-up ads to the browser and apps in the dashboard to try to sell us more products, just like they do on our laptops and phones. The difference is that a laptop infected with a computer virus or malware is less scary than a car infected with the same issue.

³ Hackers Remotely Kill a Jeep on the Highway—With Me In It (*Wired*, July 21, 2015)

⁴ Chrysler recalls 1.4 million hackable cars (*CNNMoney*, July 24, 2015)

⁵ Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits (*Federal Bureau of Investigation*, March 17, 2016)

⁶ The FBI Warns that Car Hacking Is a Real Risk (*Wired*, March 17, 2016)

**@YourCar:
“Loading a software
security patch for
infotainment system.”**

The stakes for data security are raised when we start bringing self-driving cars into the equation. In May 2016, a driver was killed in an accident that occurred when a car was under the guidance of an autonomous feature.⁷ As control of the vehicle moves from human to machine, it becomes more important than ever that data security cannot be compromised.

KPMG’s 2013 study, “Self-Driving Cars: Are We Ready?” revealed that safety and trust will play a huge role in the market for self-driving cars. The consensus among many consumers we interviewed was that computers, smartphones, and GPS devices regularly malfunction, so why not autonomous vehicles? They also said they trust technology companies more than even premium auto brands when it comes to self-driving cars.⁸

Ensuring data availability is also a huge concern. Today’s high-tech vehicles use data to drive, provide feedback, connect to other cars, and manage the lives and activities of their drivers and passengers. Lost or compromised data can cause breakdowns in all of these processes, which can inconvenience or even endanger consumers. For example, if consumers are not being fed the music recommendations they want or if service alerts are not popping up when they are supposed to, they are likely to blame the automaker.

Today, an average midsize vehicle has approximately 40–50 individual microprocessor-driven systems requiring 20-plus million lines of code. Compare that to a Boeing jet, with 15 million lines of code.⁹ Amid such complexity, it is easy to see how data flows can breakdown, and when they do, it hurts the brand reputations of the automaker. For example, infotainment systems were once one of the biggest factors in buying a vehicle, and malfunctioning infotainment systems led to less favorable ratings on *Consumer Reports Reviews*.¹⁰

Data privacy

With greater connectivity and integration between the connected car and other devices and systems, cars have access to volumes and volumes of information, and automotive companies must ensure the data is collected,



“Auto manufacturers and OEMs are starting to offer bug bounties, inviting hackers to hack their vehicles, and if successful, they are paid a fee. This open-source approach permits the manufacturers and OEMs to identify vulnerabilities.”

—Ron Plesco, Principal and National Lead, KPMG Cyber Investigations

⁷ Fatal Tesla Crash Won’t Slow Federal Push for Autonomous Cars (*Car and Driver*, July 21, 2016)

⁸ *Self-Driving Cars: Are We Ready?* (KPMG, 2013)

⁹ *Me, My Car, My Life* (KPMG, 2014)

¹⁰ Brand-by-Brand Guide to Car Infotainment Systems (*Consumer Reports*, June 2, 2016)



“With greater connectivity, cars have access to all this information. Automotive companies need to make sure it’s not retained and used for inappropriate purposes.”

—Doron Rotman, Managing Director and Privacy Service Leader, Advisory, KPMG

**@YourCar:
“Dialed Dr. Garcia
at 555-321-1234 for
Passenger Alex’s blood
test results.”**

retained, and shared appropriately. Yet, there is still much uncertainty for automakers trying to address data privacy issues.

Say, a car company tracks a driver regularly visiting a cancer clinic. Should this information be hidden from health insurers but shared with medical providers? Who decides that, and how do you ensure that it is done right? Can a health insurance or life insurance company subpoena that information?

With greater connectivity and more data volume and complexity, especially with data-rich mobile devices synchronized with connected cars, automakers face a host of new questions about data usage, ownership, and collection. What data are you collecting? Are there limitations to what you can collect? Do you need consent? Are there laws or regulations that govern the data in your systems? What are the uses allowed for what data?

There is also the question of ownership. With different companies creating different components of the car, and data privacy rules always evolving, these questions are still unclear. Does the automotive company that manufactures the car have a right to claim ownership of all of the data in its network? Or does the wireless telecom provider of the driver’s mobile phone own the data? Or maybe it’s the company that provides infotainment or communication within the vehicle – OnStar, Sirius, etc.?

In April 2016, leading German business newspaper *Handelsblatt* reported that Apple—seeking an OEM partner to help it build a highly networked electric “iCar” packed with cameras sensors that share huge amounts of data with iCloud—saw its negotiations with both BMW and Daimler collapse, in part over a question of data ownership. According to the report, “Apple wants the car to be closely built into its own cloud software, while the German carmakers have made customer data protection a key element of their future strategy.”¹¹ In other words, BMW and Daimler not only recognized the commercial value of data, but they also realized that if they

¹¹ *Fighting Over the Driver’s Seat (Handelsblatt, April 21, 2016)*

do not integrate privacy into their considerations and build it upfront, they may end with a conflict between their business plan and regulatory requirements.

Speaking of which, regulation is also big factor in data privacy. Automakers will need to take special precautions to protect extra sensitive, personal data that is governed by data privacy rules and comply with the laws in different jurisdictions. For example, the recently enacted E.U. General Data Protection Regulation raises the bar on the privacy standards companies that collect, store, process, and share personal information must comply with. The regulation also introduced significant potential fines for violations of the regulation—up to 20 million euros or 4 percent of a company’s worldwide revenue.

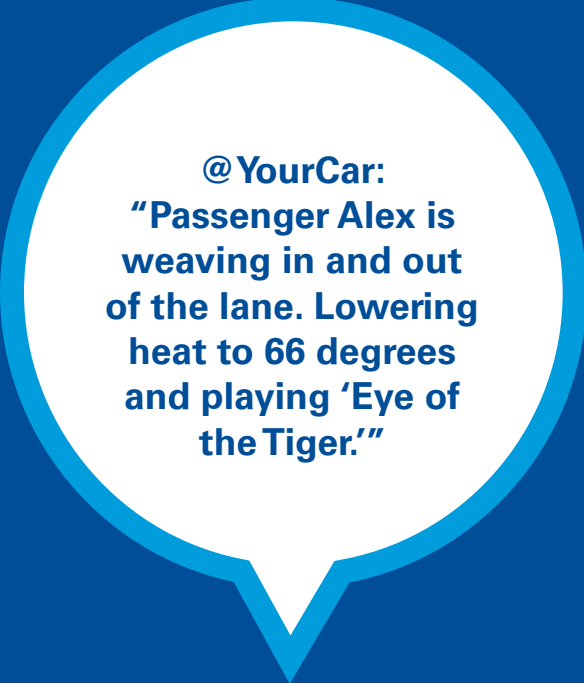
In addition, some countries, like China and Russia, have strict laws on data localization. The primary storage and processing of a citizen’s data must reside in his or her home country. If every country decides to own and protect its citizens’ data, then each OEM would need a data center for each country separate from the others, thereby changing the cost and service model, and potentially limiting the ability to leverage the data. Finally, regional and country-by-country privacy regulation could place restrictions on the movement of personal data, even data needed for service and not for marketing.

Of course, consumers regularly sacrifice data privacy for convenience. Consider electric toll collection and gas station pay passes. In the future, connected car owners may willingly give up a certain level of privacy for discounts, incentives, or the ability to share information with a social network, such as where they are driving or what they are listening to. OEMs will need the build the right privacy and security controls to allow users to choose how they want to use their data.





A closer look under the hood



**@YourCar:
“Passenger Alex is weaving in and out of the lane. Lowering heat to 66 degrees and playing ‘Eye of the Tiger.’”**

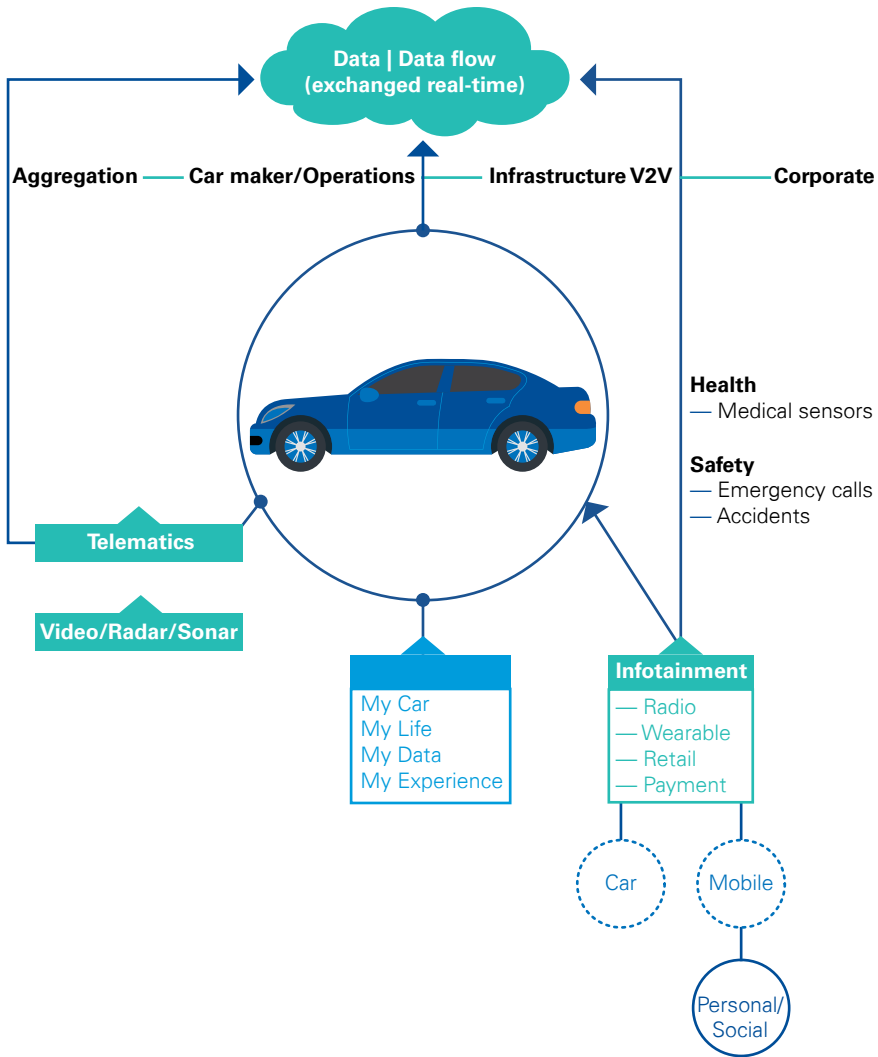
To understand how to balance risk and reward of a connected car’s data, automotive companies first need to understand how data moves from the sources of data through the vehicle, into the cloud, and back down again.

Every connected car that is manufactured today has a master onboard computer system. On average, there are more than 60 wired and wireless connections that draw data and information into the motherboard. Onboard sensors and processors measure things, such as the speed and acceleration of the vehicle. Pinpoint GPS services track the car wherever it goes. Wireless Internet access enables drivers to sync their external devices, such as smart phones and wearables (smart watches and fitness trackers). Advanced telematics and telemetry include in-vehicle security systems and tracking technologies and remote vehicle diagnostic and control technologies. Robust infotainment platforms deliver music, navigation, phone calls, and more directly to the vehicles console.

What kind of data flows through the network? Connected cars take in lots of information on the health and performance of the vehicle and its components, using sensors and telemetrics. Through the infotainment system and synced-up external devices, they can collect both personal and business-related information and communication of drivers and passengers, including credit card information; texts, calls, and e-mails; personal contacts; health information like vital signs, prescriptions, and medical histories; and consumer insights, such as browsing, shopping, and listening behaviors. Other data, collected by GPS units and tracking technologies, includes locations, routes and movements of vehicles.

So, where does all of this data go? The complexity of this question is magnified by the interconnectedness of the network to the cloud—in fact, multiple clouds. The data could land with automakers themselves in their private corporate cloud. Or, the data could go to clouds owned by content delivery systems such as music streaming and navigation, or other third parties, like advertisers, businesses or governmental organizations.

The key point is this: The OEM will be responsible to the consumer for the use and distribution of their activity data. In fact, if a consumer wants to revoke the right to use his or her data, then the OEM must be able to revoke it from all of the players in their ecosystem, meaning they must know where the data is at all times and how to manage and control it on each consumer’s behalf.



Data sources:

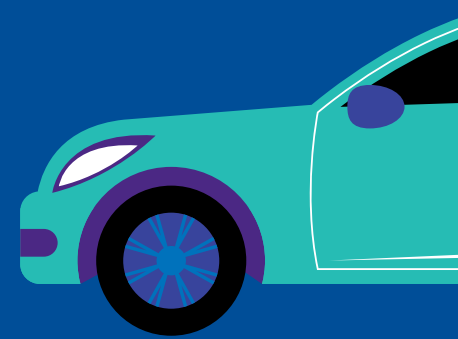
- Cabin settings
- GPS units
- Onboard sensors
- External devices, including smart phones and wearables
- Telematics and telemetry
- Infotainment platforms

Types of data:

- Personal information
- Locations and routes
- Health information
- Consumer insights

Data flows:

- OEM private clouds
- OEM monetized databases
- Government-accessible platforms
- Third-party networks





Cybersecurity in a connected car

So, for all the talking connected cars are doing—and all the data flowing back and forth—automakers must make sure the only people listening are the ones who are supposed to be listening. That is no easy task.

From a cybersecurity perspective, closed vehicle systems are much easier to secure than connected ecosystems. Not only are there more potential points of entry into connected systems, but there is also more communication happening between vehicles and third parties that must be secured. Because a connected car has an intricate web of connected systems, a breach to one system can compromise all others, multiplying the potential impact of a data breach.

What's more, cars are becoming more and more information-driven. That means there are simply greater volumes of data to protect, and the data itself is becoming increasingly personal, sensitive, and crucial to the acts of driving and traveling.

Further complicating the issue is the fact that cars were not initially designed with a secure architecture in mind. Thinking of cars as mechanical objects, automakers did not consider that one day their vehicles might provide infotainment, have external connectivity, share data with third parties, or collect sensitive information. As automakers added more and more technology components and connected them together, they knew they had to protect their systems. The easiest and cheapest way to do that? Add layer over layer, patch over patch of security across a single, flat network.

That is a problem. In an airplane, networks for different functions—flying the airplane versus playing online videos using Wi-Fi—are segregated, thus enhancing overall data security and privacy. However, in a connected car, all systems share a network, meaning if you access one you may be able to access them all. In real life, this means a hacker might be able to expose vulnerabilities in a driver's smart phone to steal information from vehicle systems the device is connected to or even take control of a car's operational systems, like its engines and brakes.

Even if the technicalities are hard to comprehend, the data risks of connected cars are apparent to consumers, regulators, and automakers. From Southwest Research Institutes Automotive Consortium for Embedded Security to the SAE Vehicle Electrical System Security Committee to the U.S. Council for Automotive Research Cyber/Physical Systems Task Force, it has prompted a slew of industry groups to pop up specifically focused on securing vehicle data, software, and systems.

**@YourCar:
"Denying access to
unknown IP address
in China requesting
access to steering
controls."**

**Eighty-five percent
of automakers admit
their organizations have
been breached in the past
24 months.**

**Two-thirds of automakers
haven't invested in information
security in the past year.**

Source: *Data Loss Barometer* (KPMG, 2016)



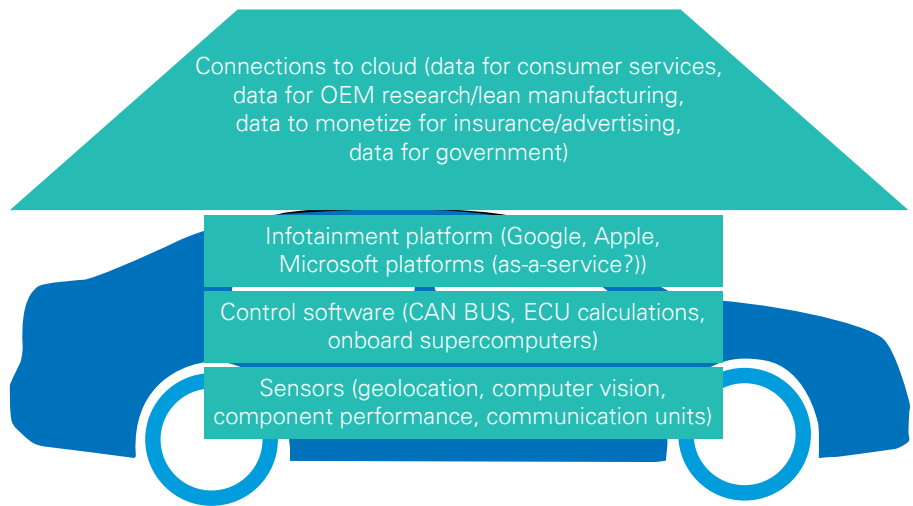
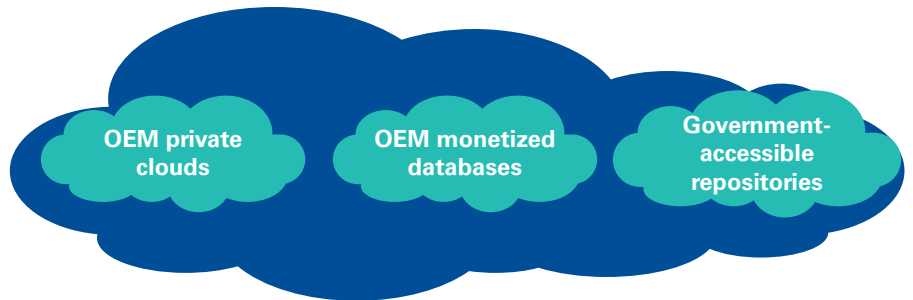
“Automakers are playing catch-up when it comes to cybersecurity, because as traditional industrial manufacturing companies, they are not used to security models for open, accessible, Internet-connected networks. While developing models and practices to meet the future needs of security will be a long and involved process, car companies today need to make cybersecurity a strategic imperative to ensure they are protecting the drivers of their vehicles.”

—*Danny Le, Principal and Automotive Leader, KPMG Cyber Security Services*



“There is little security in a connected car right now due to the nature of the way the car has been designed. The master computer system and, on average, 50 plus ECUs were engineered to be internal, except for sharing diagnostic information with the dealer or mechanic, etc.. Now you’re layering in interconnectivity to mobile devices, to apps, to satellite radio, etc. You don’t have network segmentation to separate the cars systems, like the tires and the brakes, from the infotainment system or from connected devices. That’s a security risk.”

—*Ron Plesco, Principal and National Lead, KPMG Cyber Investigations*



At each level: Which data is collected? Saved? Shared?

Reaching your data destination

So, how can companies balance the potential business opportunities presented by the data collected by connected cars with the risks that come from mishandled or compromised data?

Here are some key considerations:

Embed security and privacy at the earliest phases of product and software development.

Today, cybersecurity is too often considered a “latch on” in the automotive industry, leading to costly, disruptive fixes and course corrections, like recalls, on vehicles that are already on the road. In the future, we think cybersecurity should be integrated into every step the automaker’s developers and engineers follow as they create the software components of a connected car.

When automakers incorporate privacy and cybersecurity considerations at every phase of the software development life cycle—from presenting the initial concept to outlining the requirements for what the software will do to designing, coding, testing, and installing the software—their vehicles will be secure *by design*. Security vulnerabilities can be identified and corrected upfront, enabling automakers to avoid bigger issues down the road.

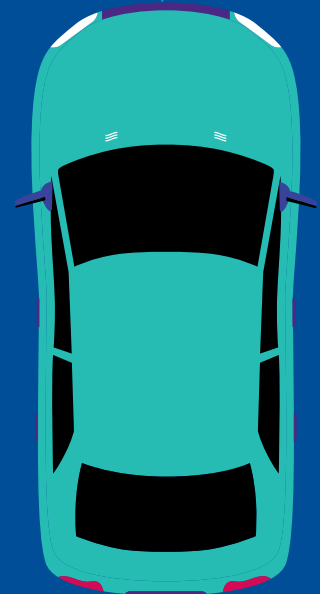
Include cybersecurity in enterprise-wide risk governance.

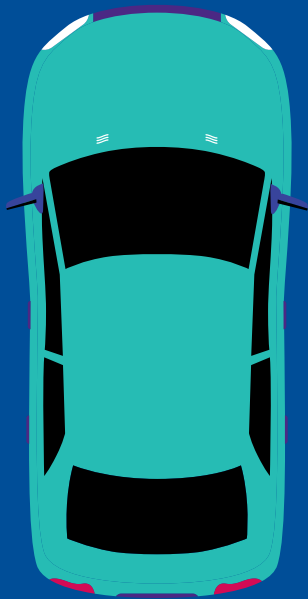
Many of the critical data security threats facing connected car manufacturers can start to be addressed by thinking of cybersecurity as a business issue and elevating it into larger risk governance conversations. Many automotive manufacturers and suppliers are in the process of building cybersecurity into an overall risk governance approach to ensure that the supply chain, design, and manufacturing process and services have cybersecurity, data privacy and protection, embedded into the whole life cycle. Further, the industry is hiring business consulting firms to assess, design, and implement this governance approach.

The evolving ecosystem of connected devices is creating significant challenges with developing and building responsibly secured devices in an environment where new threats frequently appear and boundaries are difficult to define. Organizations seeking to build preventative and detective measures around connected vehicle risks must create a responsibly connected vehicle program using a holistic approach of providing governance and oversight—from business strategy decisions to ongoing risk management.

Whether they develop cybersecurity capabilities in-house or acquire them from external parties, we think automotive companies need to increase their knowledge and skill in key areas, like information assurance and forensics. Building a security operations center, a central unit that deals

**@YourCar:
“Parked at office.
Scheduled heat system
to warm up just before
Passenger Alex’s lunch
break at 11:50 a.m.”**





with security issues on an organizational and technical level, is a good starting point.

Focus not just on the data but also on the entire ecosystem.

In a connected car, there is data flowing not just through the car but also throughout an entire ecosystem. That includes data collected by the car and shared with third parties, as well as data coming into the car from the cloud.

This data is analyzed by many different ecosystem participants for different purposes with different service levels. As such, the entire ecosystem must be secure and coordinated, and the quality of all the data within it must be reliable and accurate.

As such, OEMs must look beyond the car. OEMs should engineer and own the security of user and automotive data coming from the car. They have the unique opportunity to control the standard and approach of how the rest of the ecosystem will use and exchange the car's data.

OEMs must invest in this capability. If the OEM does not control this standard, then they may be vulnerable to other parts of the ecosystem, which may then commoditize their role in getting this data.

Be good citizens when it comes to customer data privacy.

As cars become more connected, it is fair to say that almost every action they take can be tracked, recorded or shared – even if owners of those cars don't really think about it or even truly understand it. Therefore, it is up to the automaker to ensure customer data is managed responsibly and appropriately.

Automotive manufacturers must strive to provide total transparency about what data is collected and how it is used. They should provide appropriate notice to customers about any changes in data privacy practices. They should allow consumers to opt in or out—to choose when they share their data and with whom. And they should also voluntarily follow auto-industry privacy guidelines, as several have already done.¹²

Remember: Always keep in mind customers' expectations for privacy and limit the use of data only to what customers both expect and accept.

Remember the three tenets of data security.

As mentioned earlier in the paper, the three tenets of the NIST information security standard are confidentiality, integrity, and availability. Confidentiality

¹² [Connected Cars: Dealing with data privacy \(Telematics Wire\)](#)

is the ability to obfuscate data and make it hidden. Integrity is making sure it does not change without permission. Availability is the ability to access it when needed.

At KPMG, we believe securing the Internet of Things, including connected cars, requires control, privacy and trust, which can be achieved by balancing confidentiality, integrity and availability of data.

Prepare for emerging security risks.

Technology is ever changing, and with every technological change comes new security risks. Automakers should look around the corner to anticipate what security risks might arise tomorrow.

For example, companies are just beginning to enable over-the-air updates for connected software, such as adding a software patch to a software node on your tires, similar to the simple, transparent, instant way you update apps on your smart phone when Apple or Samsung prompts you to. This is a thrilling possibility for today's automakers, which are focused primarily on making sure every software component connects seamlessly back to the master computer. However, they need to think deeper, realizing that every such software update presents a cyber risk. Can the update be done on a landline? Over Wi-Fi? Does it require a secure line? Should the data be encrypted?

Encrypt information coming into the master computer.

Cybersecurity successes and failures are largely dependent on how vulnerable the car's master computer system is. As such, we think automakers should consider encrypting data from external devices that talk to the master computer, i.e., inputs from the person using the car and his or her passengers.

Manufacturers should realize that encryption will add costs to the cybersecurity program, and it could also cause a system bandwidth issue, given that encrypted data is bigger than unencrypted data. However, we think it may be worth the investment and can be used as a "security differentiator" in protecting and advancing your brand around data privacy and protection, safety and reliability.

Test vulnerabilities.

Consider hiring hackers to expose security flaws in connected cars. Fiat Chrysler and Tesla Motors both offer a bounty—a financial reward of thousands of dollars—for hackers who successfully exploit a security flaw and a deliver a report back with all of the details on how it was done.¹³ We think the rest of the industry should follow suit.

¹³ The automotive industry should enlist hackers to aid in cybersecurity, panelists say. (*Automotive News*, July 22, 2016)



"From a privacy perspective, the issue of data ownership is at best blurry. If you own your car, who owns the data in your car? For instance, you don't own the software in the car's ECU's because it's proprietary, copyrighted and belongs to the OEMs and manufacturers."

—Ron Plesco, Principal and National Lead, KPMG Cyber Investigations



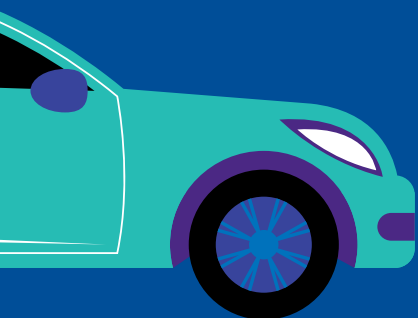
"Given the rapid pace of technology changes, tax planning should be considered with respect to all new innovation or business changes as existing tax planning strategies may no longer be aligned with the newer technologies."

—Steven Davis, Principal, International Tax, KPMG



“Privacy, as well as security and value, are critical elements of consumer trust. Connected car manufacturers must balance all three to get consumers to believe in – and to buy – their product.”

—Doron Rotman, Managing Director and Privacy Service Leader, Advisory, KPMG



Such programs generate extensive learnings on the security vulnerabilities in vehicle software, which the automaker can use to understand emerging cyber threats and weaknesses in its software.

Put safety first.

Car makers were designed, first and foremost, to bring safe, reliable, quality products to market. Safety and reliability are what consumers expect from OEM brands. While customers might settle for a car that cannot send a voice text from the in-vehicle dash, they will not settle for one that breaks down with no warning, directs a driver into a dangerous situation, or turns over control of the brakes to a cybercriminal.

In other words, the connected car discussion cannot be all about whiz-bang features and the “coolness” of the center console. The Internet-connected telemetric sensors inside a car’s mechanical and electrical systems are arguably more important, because they have the power to prevent an accident.

Therefore, we believe OEMs should focus their efforts on using connected vehicle telemetry data to reinforce and extend their core brand strength, ensuring the physical safety of their users above all else. For example, telemetry data can enable automakers to monitor vehicle systems in real-time, deliver alerts and dashboard warnings, and detect issues down the road while the car is in motion. To protect a family in a car, OEMs need to not only own that data but also expertly manage and secure that data.

Build a “three-legged stool.”

Like any new technology, it is all about consumer trust. If people trust their connected car—to keep them safe, to make their lives easier, and to treat their information appropriately—they will be happy customers. Consumers will not willingly give up their information to connected cars if they do not get anything back, such as help getting from place to place faster or assistance seeing three cars ahead. Likewise, they expect that their data will remain private and secure – that a bad actor cannot use it against them and that the wrong people will not know things about them that they don’t want them to know.

Therefore, we think automakers should view consumer trust like a three-legged stool. The legs of the stool are value, security, and privacy. If the automaker creates a connected car that is missing one leg of the stool, it will eventually topple. However, if it successfully provides all three, the stool will be stable will for a very long time.



About KPMG

KPMG's Automotive team understands the complexity currently flowing through the industry. We leverage our deep industry insight and our hands-on experience to help automotive companies shape a successful future while strengthening performance today. Using a cross-functional approach, KPMG's Automotive team helps empower some of the world's leading manufacturers, OEMs, and suppliers to achieve their goals. We put our breadth of experience and industry-specific knowledge to work with our clients, guiding them to make better decisions today to potentially create the greatest impact tomorrow.

Contacts

KPMG AG

Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch/forensic

Nico Van der Beken

Partner
Head Forensic Technology

+41 58 249 75 76
nvanderbeken@kpmg.com

Matthias Bossardt

Partner
Head of Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

©2016 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss legal entity. All rights reserved.