KPMG

Driving trust: Consumer privacy and automotive manufacturers

kpmg.com

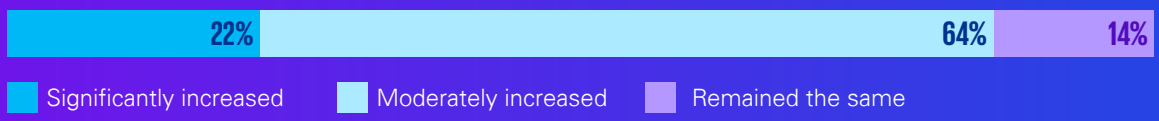
Welcome

For years, regulated industries have been under pressure to uplevel their capabilities around the ways they protect and use consumers' private information. In the automotive industry, companies have more sensitive data available to them than in the past, and they are newer to finding the right balance. As privacy and security professionals—and as drivers ourselves—we wanted to learn more about the auto industry's attempts to do the right thing for customer privacy.

We explored how automakers are thinking about customer privacy with a survey of 50 leaders from around the globe and a series of interviews with privacy leaders at global automakers. We heard that balancing data-driven innovation with customer and regulator concerns about collection, usage, and sharing is a significant undertaking that is underway with automakers across the globe. You'll find what they're already doing and our insights on leading practices to manage sensitive automotive data throughout this paper.

Privacy program budget changes[1]

Budget change over the last 12 months



Although there are opportunities for improvement, the automotive industry is heavily invested in improving data protections for consumers. We found that appropriately protecting customer privacy is a top priority for automakers, and we expect continued maturation as they learn from their own experiences and those who came before them.

We hope you find this paper helpful, and we look forward to your feedback.

Orson Lucas
Principal, Advisory
US Privacy Services Leader

Caleb Queern
Managing Director, Advisory
Automotive Cybersecurity Leader

[1] "Driving trust: Consumer privacy and automotive manufacturers," KPMG LLP (US), 2024.

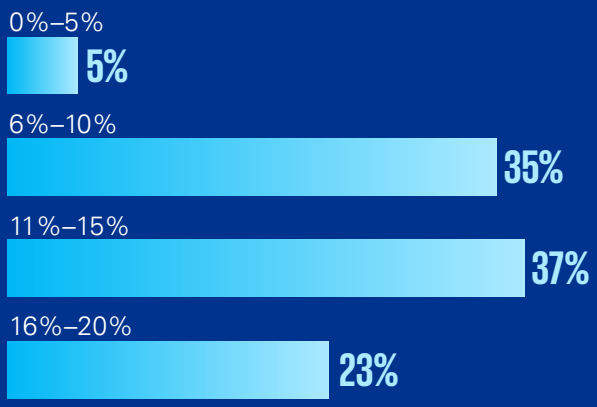
Introduction

For original equipment manufacturers (OEMs) in the automotive industry, the customer experience across marketing, sales, and service is deeply intertwined. Data-driven technologies have disrupted the ways people drive and maintain their vehicles, and there's no question that customers want the added safety and convenience that connected cars bring.[2] However, the personal data that connected features collect, use, and share is a concern for industry watchers,[3] and regulatory scrutiny appears imminent.[4] Customers don't always like what they see either. In fact, 81 percent of US adults are concerned and confused about how their data is being used.[5]

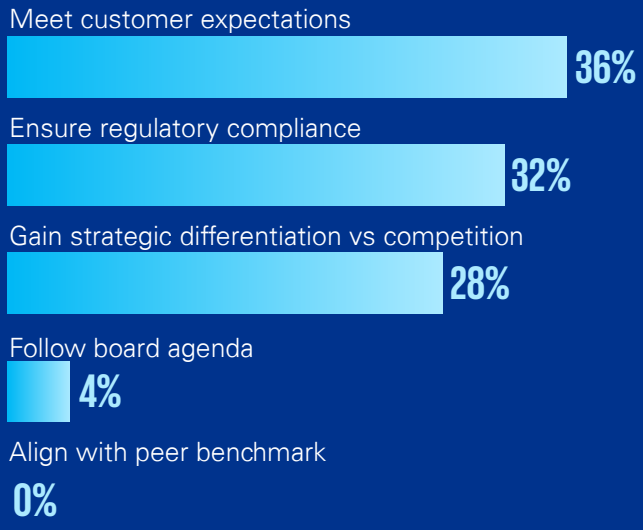
So where does that leave OEMs? At the crossroads of innovation and privacy, where connectivity, data collection, and usage are complicating customer relationships. OEMs, under increasing pressure to improve their data governance practices, are heavily invested in protecting consumer privacy. Our 2024 KPMG LLP (KPMG) study found that 98 percent of OEMs surveyed have established structured programs, frameworks, and defined roles to manage sensitive customer vehicle data. They're also planning for a privacy-centric future: 86 percent of respondents say they have significantly or moderately increased their privacy program budgets.[6]

OEMs are maturing their privacy practices, yet there is even more opportunity. OEMs can grow customer trust and satisfy regulators by implementing practices known as privacy by design and privacy by default, following ethical data policies, and using the right secure technology. In this paper, we will examine how rethinking data collection, usage, and sharing will help OEMs stay in front of evolving regulations, gain first-mover advantage, and create a competitive differentiator.

Budget increase over last 12 months[7]



Justification for investing in customer privacy programs[8]



[2] "Why the future for cars is connected," Alfalahi, World Economic Forum, July 8, 2021.

[3] "'Privacy Nightmare on Wheels': Every Car Brand Reviewed by Mozilla—Including Ford, Volkswagen and Toyota—Flunks Privacy Test," Mozilla, September 6, 2023.

[4] "Data privacy regulations continue to evolve," Vanhulle, Automotive News, June 28, 2022.

[5] "How Americans View Data Privacy," McClain, Faverio, Anderson, Park, Pew Research Center, October 18, 2023.

[6] Ibid.

[7] Ibid.

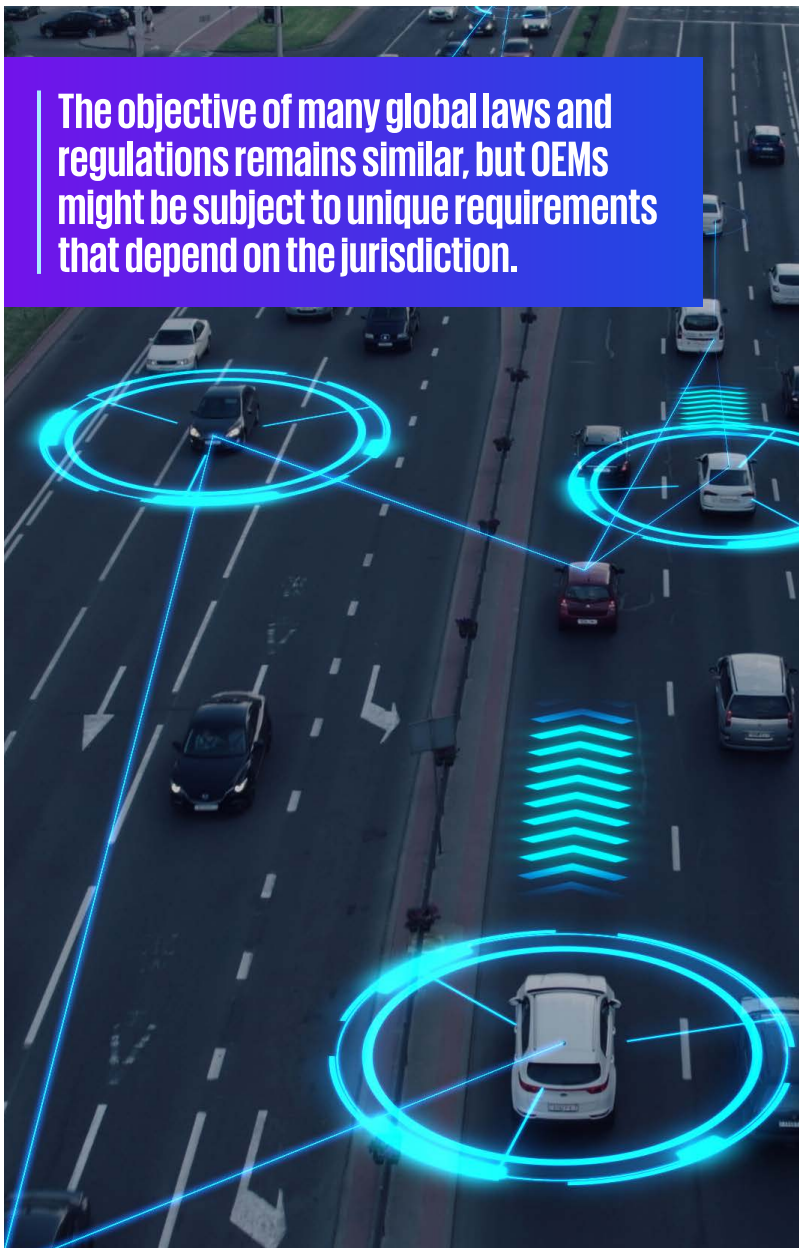
[8] Ibid.

Setting the stage: What's expected of OEMs today

To differentiate themselves from competitors on data privacy and relieve ethical concerns around data collection and use, OEMs must deliver a proactive, engaged, and transparent experience. At a minimum, that requires compliance with US and global privacy regulations today and in the future. These regulations are rapidly evolving, with over 130 countries—including the US—enacting privacy laws, with the potential for more auto industry-specific regulations in coming years.[9]

The objective of many global laws and regulations remains similar, but OEMs might be subject to unique requirements that depend on the jurisdiction. In the US, for example, several federal and state agencies and laws regulate and monitor companies' data collection, sharing, and governance processes. These include, but are not limited to, the National Highway Traffic Safety Administration's (NHTSA) guidelines and regulations. The Driver Privacy Act of 2015 is directly relevant to data from a vehicle and who has access to it. The Driver's Privacy Protection Act is a federal law that protects the privacy and personal information of customers. And at the state level, California set the tone with the California Consumer Privacy Act and the California Privacy Rights Act—these regulate organizations, including those in the automotive sector, that collect or process the personal data of state residents. Also in California, the recently passed Senate Bill 296 governs the privacy of in-vehicle camera images and videos.

The objective of many global laws and regulations remains similar, but OEMs might be subject to unique requirements that depend on the jurisdiction.

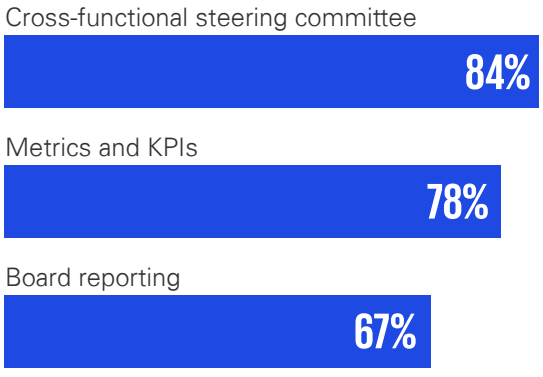


[9] "Cars & Consumer Data: Unlawful Collection & Use," Federal Trade Commission, May 14, 2024.

For countries within the European Union, the General Data Protection Regulation (GDPR) is the primary regulation affecting how data is collected, stored, processed, and shared by companies, including those in the auto industry. GDPR places strict requirements on individual consent, user rights (such as the right to access and the right to be forgotten), and data breach notifications. Companies are also obligated to perform due diligence when onboarding third parties, including signing agreements that help ensure they process personal data in the same manner as the principal organization.

In China, where data privacy and sharing regulations are strict, the Personal Information Protection Law and the Data Security Law supplement 2016's Cybersecurity Law. In addition to obtaining consumer consent, companies must also perform certain security evaluations and comply with data localization requirements before transferring personal data out of China.

How OEMs govern customer privacy efforts[10]



These are just a small sampling of domestic and international privacy laws. Proactively addressing these laws requires effective horizon scanning as well as system and process harmonization across diverse jurisdictions. OEMs are responding to the tightening privacy landscape with formal governance programs that provide rigorous analysis of their data practices. Our survey found that although only 42 percent of OEMs surveyed employ a chief privacy officer to oversee systemic handling of sensitive data, most respondents rely on other types of programs. These include cross-functional steering committees (84 percent), board reporting (67 percent), and key performance indicators (KPIs) and metrics (78 percent).

[10] Ibid.

Privacy risk exposure in the auto ecosystem

Expanding technological capabilities are increasingly turning connected vehicles into computers on wheels. But as increasingly powerful features such as geofencing and driver tracking proliferate, so does the potential risk to customer privacy. To balance innovation with privacy rights, OEMs will need to closely analyze and develop a strategic approach to in-vehicle data collection, third-party app integrations, and data handling practices.

96% **of organizations polled indicated that they conduct internal and external reviews to assess the effectiveness of customer vehicle data controls[11]**

[11] Ibid.

Consider the numerous ways vehicles use consumer data every day. Infotainment systems collect and store information about personal preferences, contacts, and communications. GPS systems track and save location histories, creating a detailed log of a vehicle's movements. Connected features extend this capability further by transmitting this data for various purposes, from traffic management to vehicle diagnostics and, sometimes, insurance and law enforcement.

Financial data could be at risk, too. OEMs increasingly offer enhanced services through third-party apps from the vehicle, such as payments for music streaming, tolls, and parking. These tools, while convenient for customers, often require access to sensitive personal data that map financial information to location and vehicle usage patterns.

Basic strategies to mitigate privacy risks across the ecosystem

The following are select actionable strategies that can help OEMs enhance privacy and build consumer trust:

Empower users to manage their own privacy settings within vehicles and mobile apps

Give users the ability to easily control what data is collected, how it's used, and where it's shared. These controls, coupled with clear and accessible privacy policies, empower users to make informed choices about their data, enhancing privacy protection and increasing user autonomy.

Ensure clarity around data sharing agreements

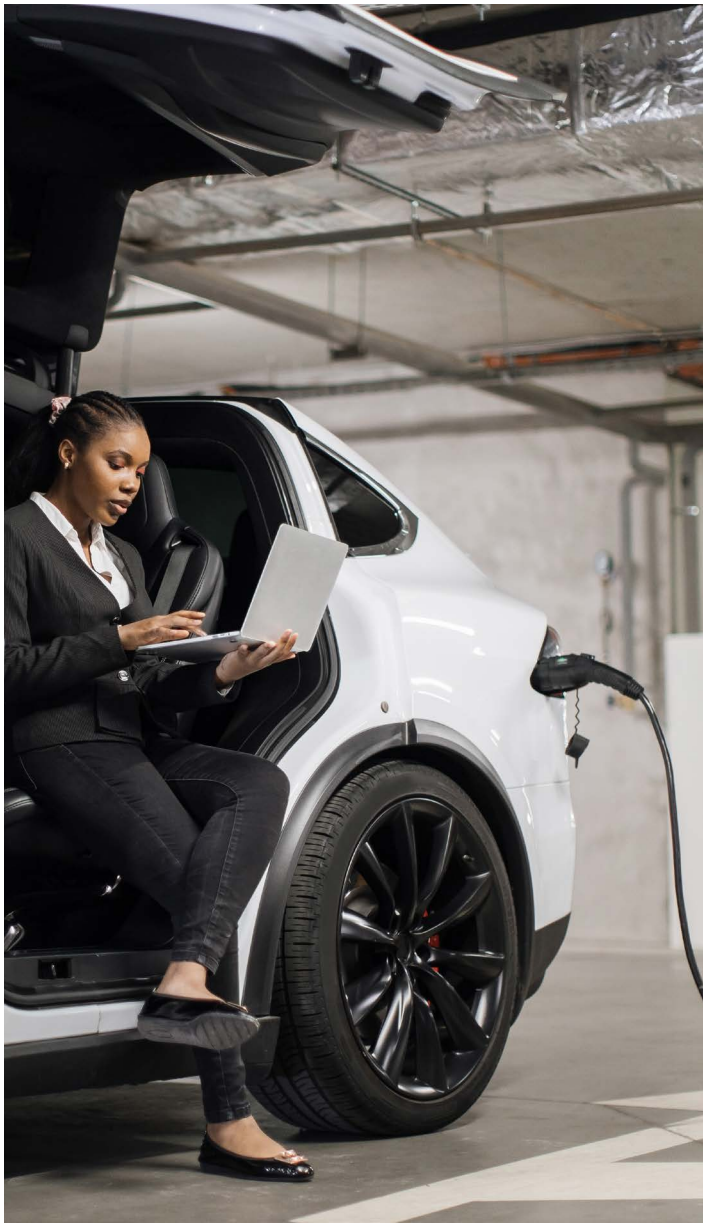
Data sharing agreements in third-party integrations should be clear and transparent. These agreements should detail third-party scope of data access, the purpose of data use, and the measures in place to protect data collected by the vehicle and associated mobile app. User privacy depends on fairness and transparency, setting clear boundaries on data usage, and preventing misuse.

Standardize data security protocols across the internal and extended third-party ecosystem

Encryption, access controls, and regular security audits ensure all stakeholders adhere to the highest standards of data protection. Such standardization helps reduce the likelihood of data breaches and unauthorized access.

Privacy by design and privacy by default

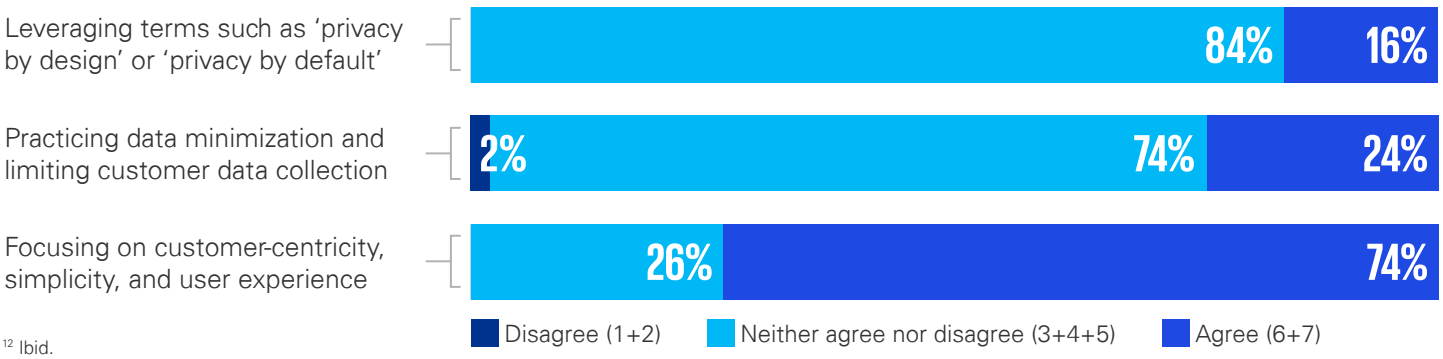
> **“As a company, we have lofty ambitions when it comes to really evolving the customer experience. That includes every touchpoint they have with the brand.”**
>
> — Leading Japanese automaker



Privacy by design and privacy by default offer a blueprint to proactively incorporate privacy best practices into products like connected vehicles. Privacy by design ensures privacy risks are understood and mitigations are built in from the start of product development. Privacy by default is an extension of privacy by design; it means that the default product configurations are the ones that offer the most privacy. Less private configurations are only possible when actively selected by users.

When integrated simultaneously, privacy by design and privacy by default enable OEMs to deliver transparency, build trust with customers, and differentiate their offerings from peers. However, although 74 percent of survey respondents say they are focused on customer centricity, simplicity, and user experience when it comes to privacy (and 82 percent say they follow a proactive approach to protect customer privacy), only 16 percent explicitly employed “privacy by design” or “privacy by default” as a strategy to accomplish that goal.[12]

Customer privacy, centricity, and data utilization[13]



[12] Ibid.

[13] Ibid.

The key principles of privacy by design include:

Integration of privacy from product inception

Privacy principles inform the development process from the very inception of projects, requiring a forward-thinking approach. In the automotive industry, this could involve designing vehicles and associated services in ways that minimize data collection, anonymize collected data, and incorporate end-to-end security measures such as data encryption. Prioritizing privacy into design choices from the earliest stages can significantly mitigate risk and ensure it's not an afterthought, which enhances consumer trust. Privacy, legal, products, marketing, and IT/security teams should be involved throughout the design, assessment, and development lifecycle (and before testing with live customer data commences). Done correctly, this not only helps limit regulatory risk but also enhances engagement with customers and increases customer trust.

Implementation of privacy-conscious design choices

OEMs can adopt anonymization techniques to ensure that the data they collect from vehicles cannot be traced back to individuals. An example is the use of differential privacy, allowing for the collection of useful data without compromising the privacy of individual customers. Additionally, designing vehicle systems to perform data processing within the vehicle itself—rather than sending data to the cloud—can minimize the impact of data breaches.

Privacy by default entails:

Implementing maximum privacy settings at the start

Privacy by default is an essential component of privacy by design. It emphasizes that systems and products should only collect the minimum amount of data necessary for their intended use, with maximum privacy protections as the default (requiring customers to have to modify settings to be more permissive). This delivers the privacy that most customers likely desire without requiring additional actions on the part of the customer, a practice that can significantly enhance trust and confidence. In the context of connected vehicles, this could mean that default settings are configured to prevent or limit data collection and sharing, thereby safeguarding user data from the outset. For example, a connected car might come with location tracking services turned off by default; users would need to opt in to access navigation. These controls should be clear, unambiguous, and easily accessible, allowing users to adjust their privacy settings, such as data sharing preferences and location tracking options, according to their comfort levels.

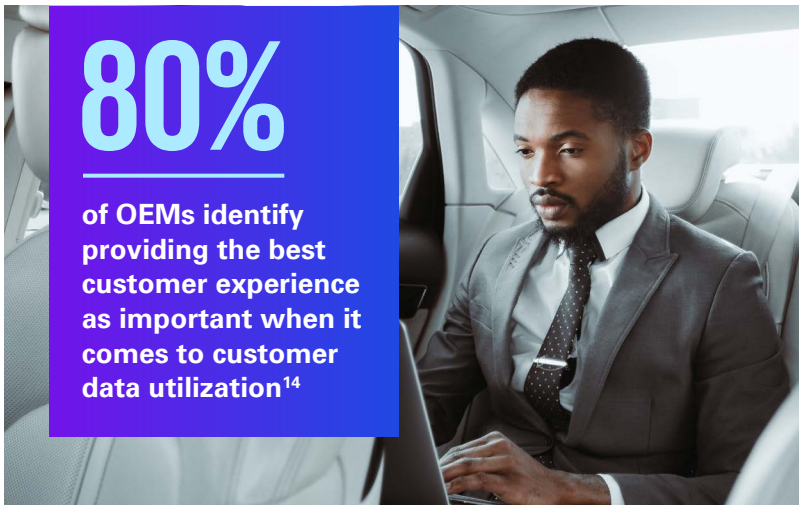
Privacy engineering translates the principles of privacy by design and privacy by default into practical, technical solutions. In developing connected car features, careful consideration of data flow, storage, and processing helps ensure that personal information is protected against unauthorized access and breaches.

By embedding privacy across the product lifecycle, OEMs can tangibly impact consumer trust, reduce the risk of costly penalties, and simplify the process of demonstrating compliance to regulators and stakeholders. Done right, these practices can also reduce the need for retroactive fixes or redesigns, allow OEMs to focus on innovation, and deliver stronger customer relationships.

Aside from incorporating privacy considerations from the outset of design, key practices include adopting a privacy-first culture, designating privacy champions within the organization, and providing comprehensive training. Additionally, conducting privacy impact assessments and data protection impact assessments can help OEMs identify potential risks early in the development process. Regular audits and continuous evaluation of organizational practices help maintain a robust privacy posture.

Balancing privacy and innovation

It's clear that connected cars can bring convenience, personalization, and safety benefits to customers. But when it comes to collecting and using sensitive data, the industry must weigh the benefits of innovation against the potential impact to customer privacy rights. In many cases, there is significant benefit to be gleaned from collection and use of sensitive data (including an end product that is potentially more compelling for some customers), but it is important for OEMs to manage this within the bounds of customer privacy preferences.



Balancing convenience and safety with privacy isn't easy

By understanding and analyzing the data collected from a variety of sensors and systems, connected cars can tailor driving experiences to make travel safer and more streamlined. For example, sensors can detect when a driver's eyes wander from the road, alerting them to pay attention. Identifying frequently traveled routes can create personalized navigational assistance that avoids traffic and road hazards. Customers can enable voice and text communications by linking their mobile device to their vehicle, helping them connect with loved ones quickly. And, in case of an emergency, some cars can automatically call for roadside assistance, providing the location and condition of the vehicle to expedite response time, potentially saving lives.

Connected cars can also harness data to optimize performance and resource consumption. These vehicles can analyze engine performance, driving style, and other car-related metrics to provide tailored feedback to customers, promoting environmentally friendly and economical driving habits. Also, predictive maintenance alerts powered by real-time data analysis can prevent breakdowns and unnecessary repairs, saving resources and extending the lifecycle of the vehicle.

For their part, customers may not be aware what data is being collected and used, and gaining user-informed consent isn't as simple as it sounds. The process must ensure that customers fully understand when and what data is being collected, why it is being collected, and how it will be used or shared. Consent (opt-in or opt-out) must be easy to understand, agree to, and written in plain language. Without clear, comprehensible, and transparent notice, there is a risk that customers may unknowingly consent to practices they do not approve of, potentially leading to a breach of trust.

[14] Ibid.

Feature	Benefit	Customers may wonder...
Attention sensors	Sensors detect and alert when a driver's eyes wander from the road	Is that data included in the data shared with my insurer?
Location trackers	Convenient recommendations from mapping applications	Is there a way for me to block where I go in the vehicle from my estranged spouse?
Cruise control	Improved fuel efficiency	Will fuel efficiency data affect my charging rates?
Electric battery	High-speed charging saves time	If high-speed charging can reduce battery life, will my charging behavior affect my car's resale value?
Onboard cameras	Automatic driving and parking support	Will the camera capture and collect biometric information about me, my friends and family, or others? What will happen with that footage/data?
Fuel efficiency metrics	Better product design	Will my vehicle's data be shared someday with the government or environmental regulators in a way that's uniquely identifiable to me?
Tire pressure sensor data	Improved driver safety and fuel efficiency	Is this data legally discoverable after a crash?

Importance of user consent, transparency, and control over data collection and usage

As personalization increases, enabling user consent, transparency, and control in data collection and usage is crucial.

Only collect what's necessary. Avoid collecting anything beyond what is essential for services and limit the amount of stored personal data. This practice reinforces trust with customers and reduces the risk of substantial data loss if a security breach occurs.

Clearly define and communicate an explicit rationale for the purpose of data collection. This keeps collection practices in harmony with data management principles, validates the approach, fosters responsible behavior, and enhances efficiency.

Delete data when it is no longer needed. OEMs should conduct privacy impact assessments to identify and define the business purpose for collection and use, updating the company's record of processing activities to link the collection to the product. Here, there is room for improvement: Only 24 percent of respondents confirmed they are currently implementing practices such as data minimization.[15] OEMs should implement a systematic data deletion schedule that aligns with privacy regulations. This promotes transparency and increases trust because it reassures customers that their data won't be stored indefinitely.

[15] Ibid.

> **“One of the first things our engineers think about is data minimization. How can you accomplish the design purpose with the minimum amount of [personal] data? Privacy compliance has shifted left in the development lifecycle.”** — Global automaker

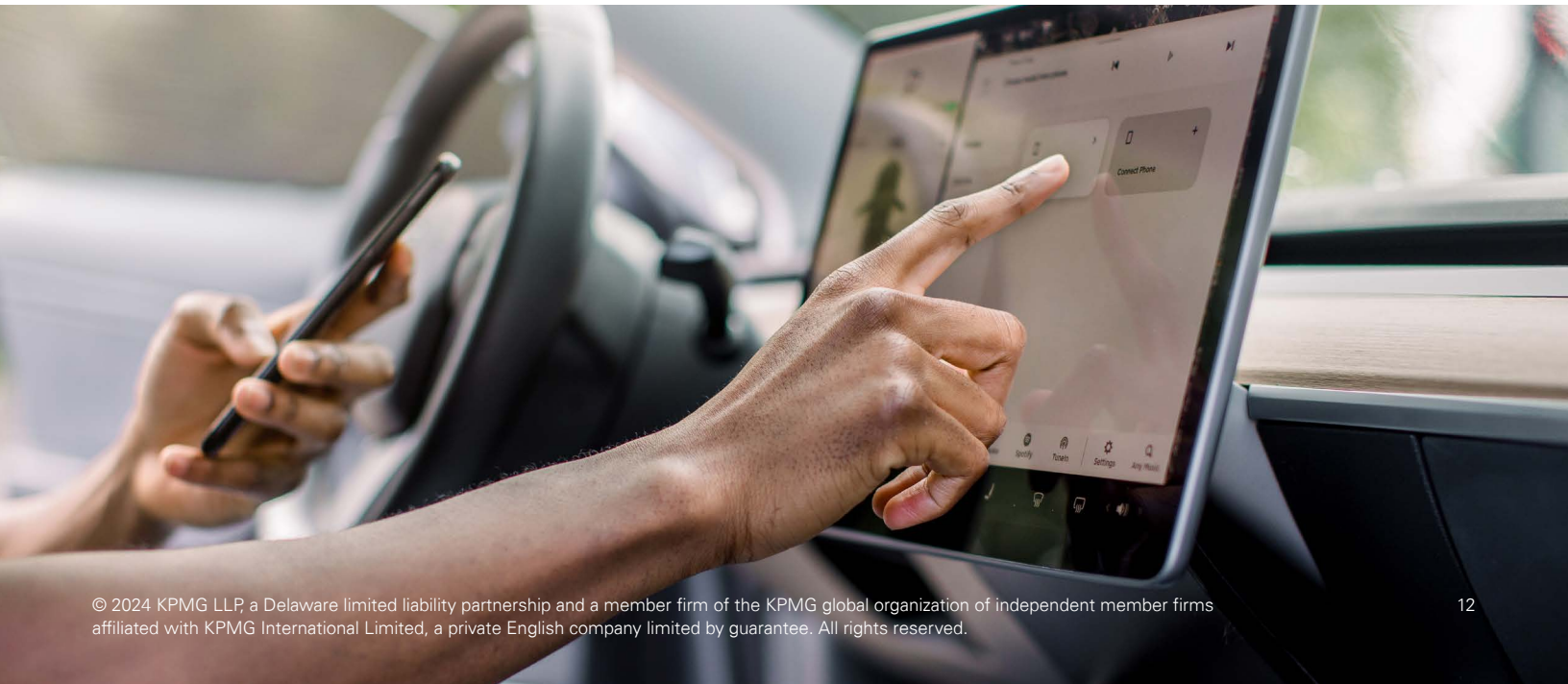
Implement customer-centric consent mechanisms. Move beyond the formality of obtaining legal consent and design a system that places the customer at the center of data collection and usage.

Empower customers with a flexible consent model. Give customers the flexibility to choose what data they wish to share, with whom, and for what purpose.

Use unambiguous language. Clearly express the action required for giving consent (e.g., “I agree” or “I consent”). Avoid preticked boxes, blanket consent, or assumed consent; instead, allow customers to provide specific and granular consent for distinct types of data and use cases. Individuals should actively acknowledge agreement by clicking a button or taking a specific action. Where possible, avoid making consent a prerequisite for use of or derivation of value from the product.

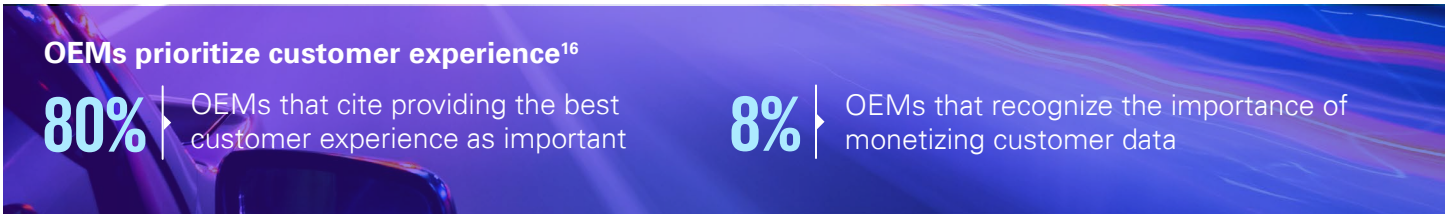
Regularly review and reassess the validity of existing consents. Inform customers about any changes in data processing practices that may affect their original consent and obtain renewed consent if necessary.

Protect individual identities with anonymization, pseudonymization, and data aggregation. In anonymization, data is processed in a way that it cannot be linked back to an individual, protecting users’ identities. Pseudonymization replaces private identifiers with fake identifiers or placeholder values. Aggregation groups data in a way that limits individual identifiability so that the individual source cannot be singled out.



Third-party data collection and sharing

OEMs understand the value of the rich data available from connected vehicles. To create broader product and service offerings, they have engaged with third parties, such as satellite radio, insurance, and navigation providers, to enhance customer experiences using personally identifiable information.



Usage-based insurance

If a customer opts in via configuration of settings in their vehicle or companion app, an OEM may share certain driving data with insurance companies. Usage-based insurance (UBI), also known as pay-how-you-drive, pay-as-you-drive, or telematics insurance, tailors pricing based on the actual driving behavior of the policyholder.

UBI is part of a broader movement toward digital and personalized insurance models, reflecting advancements in technology and changing consumer expectations. Although traditional auto insurance models determine premiums based on factors such as age, gender, vehicle type, and driving history, UBI also allows insurers to collect and assess data related to driving habits and vehicle usage, offering a more personalized insurance rate. Based on this assessment, insurers can adjust premiums to reflect risk more accurately. Safer customers who drive less frequently or during safer times of the day may receive lower rates.

Embedded telematics

Embedded telematics systems collect and transmit data about the vehicle's operation, location, and more, sending data directly to the manufacturer or third parties via embedded cellular connections. Aftermarket devices that plug into a vehicle's onboard diagnostics port can also collect and share data with third parties. In addition to UBI, fleet managers and customers sometimes use telematic devices for vehicle diagnostics or tracking purposes.

Technology companies (via smartphones) are also getting in on the game. Technologies such as Apple CarPlay and Android Auto allow cars to integrate with a driver's mobile device, effectively using the phone's data connection to access or share information. While these systems primarily aim to display information from the phone (such as navigation or music apps) on the vehicle's screens, they can also send certain types of vehicle data back to the phone, such as electric charging activity, which could then be shared with apps or services that have the appropriate permissions.[16]

[16] Ibid.

> **“If we detect drivers braking hard before a sharp curve in the road, we can share that totally anonymized data with highway authorities in an effort to increase driver safety. Just some extra signage might help reduce an accident. This will make people safer and improve the roadways.”** — Leading Japanese automaker

Mobile apps

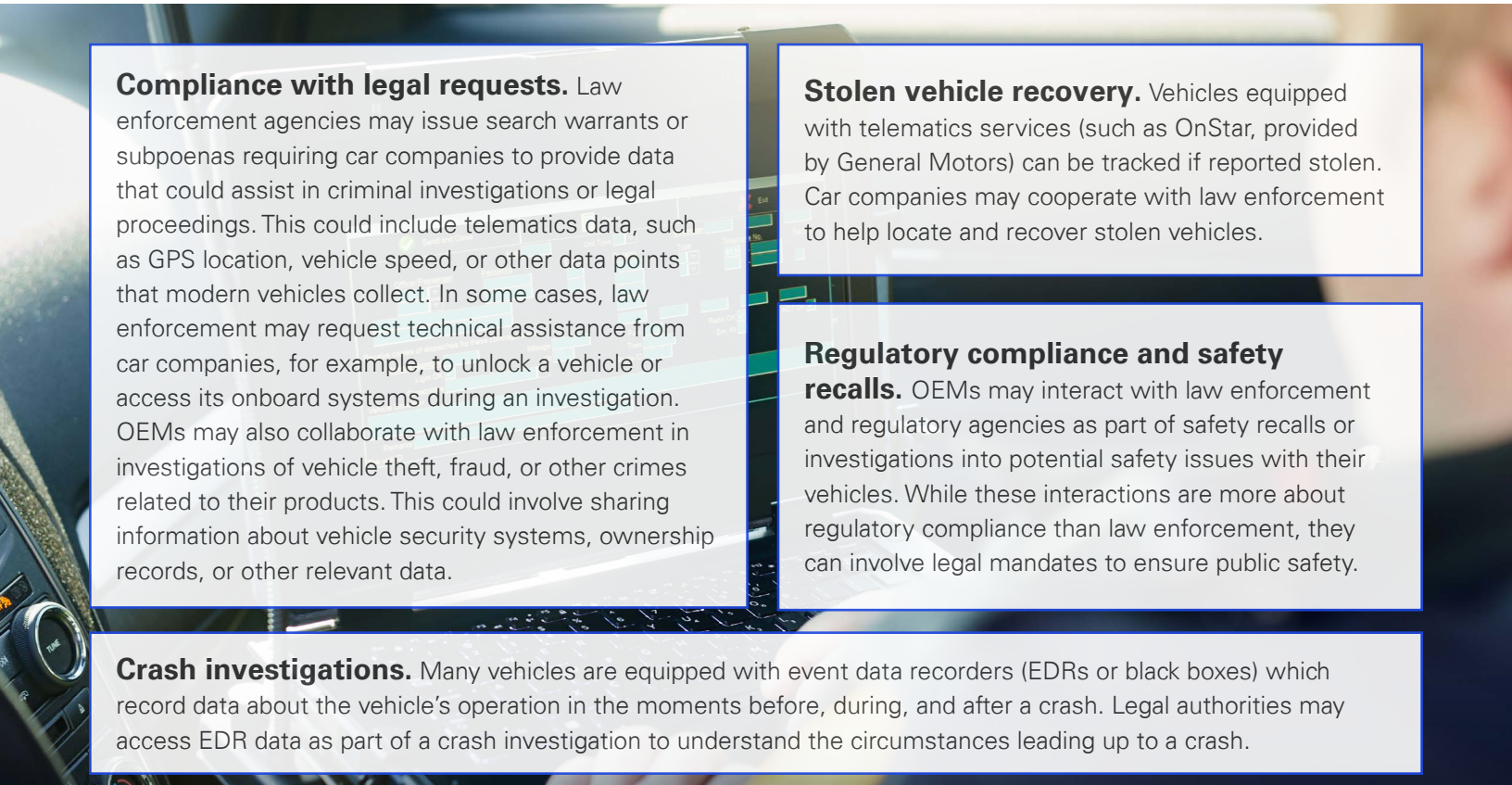
OEMs also offer companion mobile apps that connect to their vehicles for remote control (such as starting the engine or unlocking doors) and monitoring (such as checking battery status on electric vehicles or receiving maintenance alerts). These apps can collect data from the vehicle and share it with the manufacturer or other third parties.

Vehicle-to-everything communication

Vehicle-to-everything (V2X) communication enables communication with other cars and trucks and with infrastructure (such as traffic lights or road signs) to improve traffic flow, safety, and efficiency. While not yet widely implemented, V2X could share data with a broad range of third parties involved in traffic management, road safety, and vehicle services.

Law enforcement

OEMs may also share driver and vehicle information with law enforcement agencies. The nature of these interactions can vary depending on the jurisdiction, the specific legal framework in place, and the situation.



Compliance with legal requests. Law enforcement agencies may issue search warrants or subpoenas requiring car companies to provide data that could assist in criminal investigations or legal proceedings. This could include telematics data, such as GPS location, vehicle speed, or other data points that modern vehicles collect. In some cases, law enforcement may request technical assistance from car companies, for example, to unlock a vehicle or access its onboard systems during an investigation. OEMs may also collaborate with law enforcement in investigations of vehicle theft, fraud, or other crimes related to their products. This could involve sharing information about vehicle security systems, ownership records, or other relevant data.

Stolen vehicle recovery. Vehicles equipped with telematics services (such as OnStar, provided by General Motors) can be tracked if reported stolen. Car companies may cooperate with law enforcement to help locate and recover stolen vehicles.

Regulatory compliance and safety recalls. OEMs may interact with law enforcement and regulatory agencies as part of safety recalls or investigations into potential safety issues with their vehicles. While these interactions are more about regulatory compliance than law enforcement, they can involve legal mandates to ensure public safety.

Crash investigations. Many vehicles are equipped with event data recorders (EDRs or black boxes) which record data about the vehicle’s operation in the moments before, during, and after a crash. Legal authorities may access EDR data as part of a crash investigation to understand the circumstances leading up to a crash.

Best practices in third-party data management

When sharing consumer personal data with third parties, automakers should first determine an effective approach to third-party data governance. Key activities include:

01

Assessment. Conduct a thorough evaluation of potential third-party vendors before engaging in any collaboration. Examine their data protection practices, security measures, and compliance with relevant privacy regulations.

02

Engagement. Establish clear and comprehensive data processing agreements that outline the responsibilities of each party, data processing purposes, security measures, and data handling instructions. Align these agreements with applicable data privacy laws and define the scope of the agreement and the duration of the confidentiality obligations. Clearly communicate data retention policies and establish procedures for secure data disposal when it is no longer needed.

03

Monitoring. Audit third-party activities to help ensure compliance with the agreed-upon data protection and privacy standards. Regularly review security controls and conduct assessments to verify compliance.

04

Improvement. Provide training and resources to third-party collaborators on data privacy best practices, legal obligations, and security protocols to help ensure they are knowledgeable about their roles and responsibilities regarding data protection. Maintain cross-border compliance with data transfer mechanisms provided by relevant regulations. Consider ensuring an adequate level of protection in the recipient country. Regularly review and update collaboration terms. Monitor third parties' compliance with evolving privacy regulations and organizational requirements.

05

Protection. Monitor third parties' compliance with appropriate data protection and security measures, including encryption, access controls, regular security assessments, and data breach notification processes. Define roles, responsibilities, and escalation processes to handle any privacy or security breaches effectively. Establish clear incident response and remediation procedures in the event a data breach or privacy incident occurs.

Emerging role of privacy-enhancing technologies

As OEMs continue expanding the technological capabilities of their vehicles (and consumers become savvier about the ways their data is collected, used, and shared), traditional methods to manage privacy may not be enough. New privacy-enhancing technologies (PETs) such as differential privacy, secure multiparty computation (SMPC), federated learning, and homomorphic encryption will help OEMs stay ahead of the curve.

PETs	Differential privacy	SMPC	Federated learning	Homomorphic encryption
Overview	It helps ensure the privacy and security of an individual's data within a data set while still allowing for the analysis of the aggregate data. It maximizes the accuracy of queries from statistical databases while minimizing the chances of identifying its entries.	It is a cryptographic protocol that enables parties to jointly compute a function over their inputs without revealing that data to the other participants, or even to a third party conducting the computation.	It is a type of machine learning that trains algorithms across multiple decentralized devices or servers. This method allows for the creation of shared models without the need to centralize sensitive information.	Homomorphic encryption allows computation on ciphertexts, generating an encrypted result that, when decrypted, matches the result of operations performed on plaintext.
Benefits	• Privacy breaches are safeguarded, even when attackers have access to external information. • It's adaptable to various data types and requirements. • Mathematically grounded privacy guarantees build trust with customers concerned about data usage.	• Organizations can jointly analyze combined data sets without revealing sensitive or proprietary data. • Companies can securely share information without revealing sensitive data.	• It aligns with data minimization principles. • It allows for model personalization. • Heterogeneity ensures fair model training. • It has a lower risk of data breach and misuse. • It saves bandwidth and reduces latency.	• Raw, unencrypted data remains private during computation and analyses.
Challenges	• There is a trade-off between utility and privacy. • It requires expertise in statistical and cryptographic techniques. • It can be difficult for non-experts to understand.	• There are high costs for large-scale applications. • Higher security guarantees can lead to higher computational costs. • Compliance isn't guaranteed.	• There is high communication overhead. • There are heterogeneity challenges during model training and convergence. • It raises new security questions.	• There is high computational overhead. • There is increased Complexity. • It is still in development.

Summary

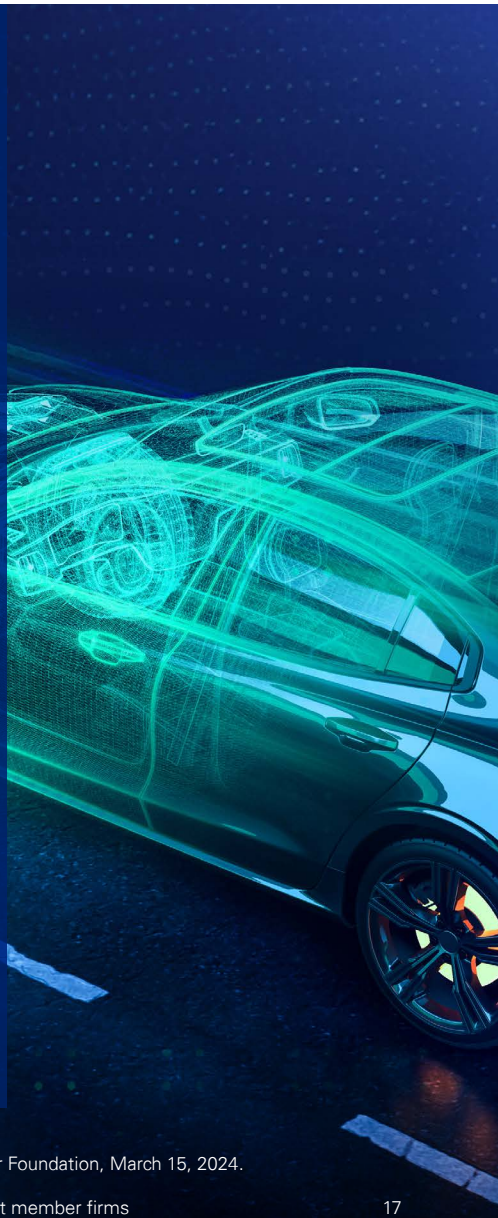
There is a growing demand among customers and regulators for OEMs to manage data ethically and securely. Our survey suggests OEMs recognize this demand and are taking steps to balance ethical collection and use of customer vehicle data. To increase customer trust and stay ahead of evolving laws and rules, OEMs should continue fortifying their privacy practices using strategies such as privacy by design and privacy by default. In the meantime, while the industry continues to mature the ways they handle personal data, customers can also take steps to proactively manage the information their vehicles collect and share.[17]

There is good reason for leaders in the automotive industry to proactively establish an early mover advantage in this area as the demand for privacy and security will increase. To develop solutions that meet stakeholders' needs, collaboration between OEMs, their partners, and policymakers is necessary to shape a future of responsible data collection, usage, and sharing.

How KPMG can help

To create experiences that regularly exceed customer expectations, businesses must be intentional about putting customers at the forefront to build their trust. By designing and orchestrating seamless and personal customer, employee, and partner experiences, organizations can improve their reputation among customers and build teams that understand the business's overarching vision.

KPMG has been the trusted adviser of organizations implementing these foundational capabilities at the regional, national, and global level across every major industry. Our deep bench of technologists, security professionals, former regulators, and attorneys brings a combination of regulatory, business process, data protection, information governance, and technology experience to help clients achieve sustainable, business-focused, flexible privacy compliance. We can help your organization navigate the evolving regulatory landscape utilizing tested and scalable privacy capabilities that inspire trust, reduce risk, and grow your business. At KPMG, our data privacy specialists work with our clients to pull together data from different parts of the organization. We coordinate with you to implement an integrated technology model that helps achieve better visibility into data collection and usage practices and more effectively operationalizes privacy as a competitive differentiator.



[17] "How to Figure Out What Your Car Knows About You (and Opt Out of Sharing When You Can)," Klosowski, Electronic Frontier Foundation, March 15, 2024.

Authors

Orson Lucas

Principal, Cyber Security Services

Orson Lucas is a Principal at KPMG LLP (US) and is based in Tampa. Orson helps complex, global organizations enhance the maturity of their data protection and privacy programs. He has been a featured speaker at over two dozen conferences and has published in leading industry publications such as Forbes, Financial Times, Compliance Week, and Bloomberg BNA. He has more than 23 years of data privacy, security, and data protection experience, and leads the KPMG Privacy Solution in the United States.

Caleb Queern

Managing Director, Cyber Security Services

Caleb Queern is a Managing Director at KPMG LLP (US) and is based in Austin. He has more than 15 years of technology and information security experience and has focused on the auto industry in recent years. His focus is reducing risk and improving performance so organizations can meet business goals and enable growth. His specialties include secure DevOps and application security, security operations, and operational excellence, and he recently coauthored Investments Unlimited: A Novel about DevOps, Security, Audit Compliance, and Thriving in the Digital Age.

Acknowledgments:

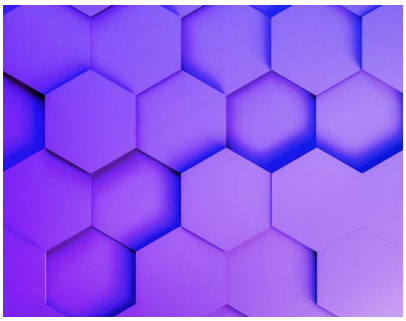
The authors wish to thank Lisa Bigelow, Matthew Caruso, Rohinish Chatrath, Gia Gustovich, Nishtha Joshi, Valeriya Kramarenko, Leah Lockwood, Kristen Manning, Brennan Morris, Rashmita Parihar, Basu Raj, and Lara Volpe for their contributions to this paper.

For more information, contact us:

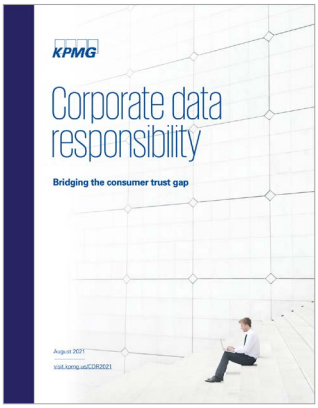
Orson Lucas
Principal,
Cyber Security Services
olucas@kpmg.com

Caleb Queern
Managing Director,
Cyber Security Services
cqueern@kpmg.com

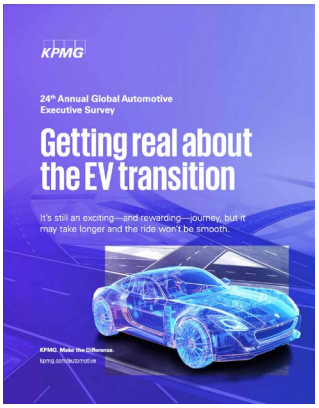
Related thought leadership:



How automakers can inspire trust in their software



Corporate data responsibility: Bridging the consumer trust gap



24th Annual global automotive executive survey

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com** **Subscribe**

DASD-2024-15954