otonomo

WHITE PAPER

A Privacy Playbook for Connected Car Data

WITH FOREWORD BY

FUTURE OF PRIVACY FORUM

Welcome

Welcome to the first privacy playbook for connected car data. When my team and I embarked on this project, my hope was to spark new avenues of discussion among the community of businesses and government organizations at the forefront of using data generated by connected cars and to produce a playbook that is helpful to business people. Throughout a career focused on data and analytics technologies, I have always advocated for the consumer voice in the data privacy conversation. I believe that one of the most important areas in technology today where it's critically important to think about consumers is connected car data.

Consumers have long considered their cars to be an extension of themselves and to be their guarantors of freedom, autonomy, and privacy. Yet, vehicle data can provide a deep view of how consumers live and what they do. In order for an ecosystem to develop around connected car data and services, both OEMs and the companies that use the data in applications and services must think carefully about managing consumer privacy—both from a legal perspective and in terms of earning consumer trust.

We are honored to have been able to collaborate with some of the brightest minds in consumer privacy. Their feedback has been invaluable to us, but we know that this playbook is only the start of a long journey. Privacy is a never-ending process, and there is no panacea of business practices or software products that instantly gets it done. We hope to continue the conversation with you—our readers—as the connected car data ecosystem evolves.

Enjoy the read, and please reach out to us with your feedback or questions!

Lisa Joy Rosner,
Chief Marketing Officer, Otonomo

Foreword

By John Verdi, Vice President of Policy, Future of Privacy Forum

Drivers and passengers expect cars to be safe, comfortable, and trustworthy. Individuals often consider the details of their travels—and the vehicles that take them between their home, the office, a hospital, their place of worship, or their child's school—to be sensitive, personal data.

The newest cars contain numerous sensors, from cameras and GPS to accelerometers and event data recorders. Carmakers, rideshare services, tech companies, and others are increasingly using data about cars to reduce emissions, manage traffic, avoid crashes, and more. The benefits of connected vehicles for individuals, communities, and society are clear. So are the privacy risks posed by increased collection, use, and sharing of personal information about drivers, passengers, cyclists, and pedestrians.

It is crucial that companies, advocates, academics, technical experts, and policymakers craft creative solutions that promote the benefits of connected vehicles while mitigating the privacy risks. Global legal frameworks have a role to play in assuring meaningful data protection and promoting trust, as do voluntary, enforceable codes of conduct and technical standards.

However, it is plain that entities must look beyond legal obligations and consider how they will earn and maintain consumer trust. With this white paper, Otonomo has taken an important step to advance the dialogue on connected car data privacy. It is vital work, and we hope it inspires the connected car ecosystem to think more broadly about data practices and to explore new ways to support consumers' trust in connected vehicles.

Executive Summary

With the advent of connected cars, new applications, services, and crowdsourced insights are emerging with the promise of making driving safer, more convenient, and more rewarding. Connected car data could have a profound impact on individual drivers as well as society as a whole.

For many use cases based on connected car data, the underlying data is personal and can only be processed in compliance with legal and technical requirements such as the European Union General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). In other use cases, the data is de-identified or aggregated, rendering it subject to different privacy obligations or not covered at all by personal data protection laws.

In either case, however, the automotive manufacturers that collect car data and any service providers using it need to consider drivers' privacy expectations when designing their data practices and privacy policies and procedures. Privacy matters more to consumers now than ever. To lead in this new ecosystem of connected car data, companies must look beyond regulatory compliance and prioritize consumer expectations and trust when building their services.

In this playbook, we present the following nine key plays that put privacy at the center of your business practices:

1. Create an end-to-end consent and opt-out signaling system that crosses company boundaries to create a seamless experience for drivers.
2. Offer consumers choices even when it is not legally required.
3. Deliver information about data collection practices and privacy in transparent, engaging ways.
4. Apply the minimal viable dataset to every situation.
5. De-identify data with the context of the use case in mind.
6. Secure car data from end to end.
7. Communicate broadly.
8. Think beyond a single vehicle owner or driver.
9. Establish a data lifecycle strategy—including disposal.

These plays will help OEMs and service providers accelerate the development of a new ecosystem for connected car drivers, one that delivers significant benefits both to individual drivers and society as a whole.

Connected cars: Ushering in a new era of transportation

Today's connected cars are becoming computers on wheels, generating data ranging from ambient air temperature and battery level to hard-braking events and road sign images, and a growing suite of services are further enhancing safety and convenience on the road. Experts predict that the transportation sector will change more in the next five years than in the previous 50 years, and we are just beginning to realize the profound impact that connected car data could have on drivers and society.

Hundreds of use cases are now emerging around connected car data:

- **Aggregate data** is being used for traffic flow optimization, mapping and planning, road hazard identification, congestion management, predictive maintenance, location intelligence, and media measurement.
- **Data from individual cars** is being shared by drivers for services delivering roadside assistance, electric vehicle charging services, subscription-based fueling, usage-based insurance, remote diagnostics, trunk delivery by retailers, and parking payments.

In the future, we will see:

- **Vehicle-to-vehicle (V2V)** communication, through which vehicles could signal their intent to each other, such as notifying several cars behind them of an unexpected hard-braking incident or electronically signaling a left turn.
- **Vehicle-to-infrastructure (V2I)** use cases, such as a vehicle reserving a parking space and parking itself or triggering a traffic light.

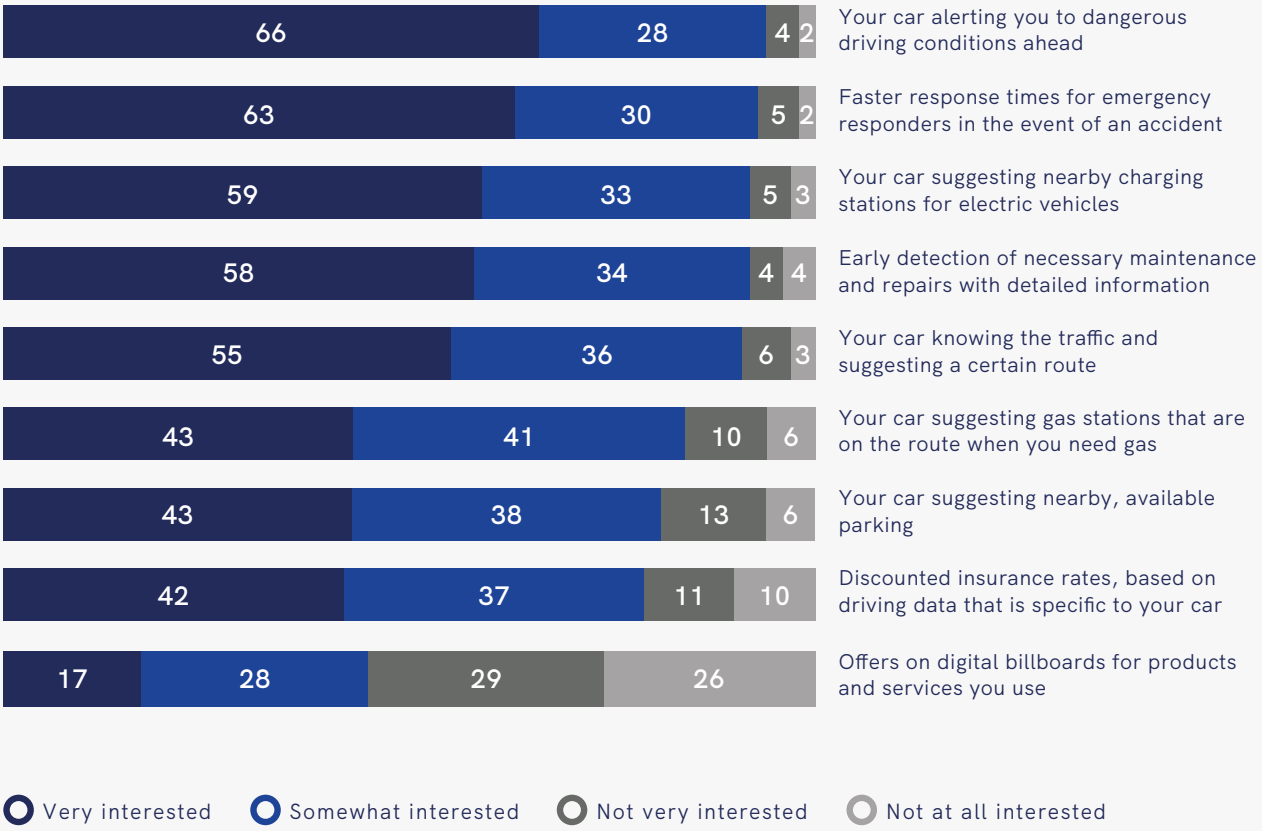
These applications, as well as other applications, services, and crowdsourced insights, will make driving safer, more convenient, and more rewarding. In addition to providing benefits to individual drivers, they promise significant societal benefits, such as reducing congestion and pollution in urban areas.

Consumers want services based on connected car data

As new services based on connected car data have become available, they are finding acceptance from consumers. In a 2018 survey of American connected car owners and new car buyers commissioned by Otonomo and fielded by Edison Research,[1] as many as 94% of respondents expressed interest in apps and services based on connected car data—even services that were not yet on the market, like delivering retail purchases to drivers' trunks.

OTONOMO-EDISON RESEARCH CONSUMER SURVEY, 2018

Drivers' interest in new apps and services based on connected car data



Approximately 80% of those who expressed interest in a number of these services (including real-time alerts of dangerous driving conditions, early detection of maintenance and repairs, and even faster response times for emergency responders in the event of an accident) stated a willingness to share connected car data to gain access to these capabilities. Similarly, a 2018 worldwide Deloitte survey[2] found that more than 70% of consumers are interested in benefits such as traffic and maintenance updates, safer travel routes, and collision detection.

Connected car use cases represent a broad spectrum of data types

For a number of the use cases we have discussed, the underlying connected car data is personal and can only be processed in compliance with legal and technical requirements such as GDPR or CCPA. Some data protection laws, such as those in Nevada[3] and California (CCPA),[4] specifically address personal vehicle data, while most do not. Automotive manufacturers (OEMs) have responded by incorporating commitments in their privacy policies and partner contracts.

In other use cases, the data is aggregated and de-identified and therefore not covered under personal data protection laws. At the same time, the data practices of OEMs and third parties may come under scrutiny. Consumers are expressing growing concerns about privacy and data protection due to events in other industries, from credit card data breaches to Amazon Alexa recording conversations without its "wake word"[5] or smart TV voice data collection that went beyond consumer expectations.[6] Privacy matters more to consumers now than ever, according to a recent survey by the IBM Institute of Business Value.[7] In the previously cited Deloitte survey, six out of ten consumers were somewhat or very concerned if data related to biometrics, data location and app usage, or driving behavior is collected and shared.

Connected car data flows

Depending on the manufacturer, a connected car may generate up to 25 gigabytes of data per hour from at least 200 sensors within the vehicle.[8] As it is produced, most of this data leaves the car via in-vehicle cellular and is initially stored in data centers or cloud platforms owned by OEMs. There are a few cases where data travels directly to tier-one suppliers, such as SiriusXM, Harman, or third parties owning onboard devices (OBDs) installed after vehicle purchase. There are no consistent formats or data standards across OEMs or even within the same OEM, so connected car data must generally undergo additional processing before it can be useful in applications and services. Companies like Otonomo have built platforms that aggregate and normalize data from multiple OEMs and perform processing to make the data more usable and valuable.

Beyond legal requirements, the connected car ecosystem must consider consumer expectations

Companies seeking to lead in the new ecosystem of connected car data must look beyond regulatory compliance and prioritize consumer expectations and trust when building their services. This may mean:

- Making it easier for drivers to exercise their legal rights
- Taking new approaches to disseminating information about data collection and data-sharing practices
- Giving drivers additional choices about how their data is used, whether or not they are legally required to do so
- Taking data protection steps that go beyond what is legally required

In this playbook, we will share some ideas for doing just that. We hope that the playbook will inspire you to look at privacy-by-design as an opportunity and not as a compliance burden.

Some caveats

This playbook is not intended to be legal advice or provide templates for privacy policies or principles such as those promulgated by industry alliances, like ACEA or the Alliance of Automotive Manufacturers. We expect that you will consult your legal counsel and Chief Privacy Officer as you adapt these plays to the unique characteristics of your business.

Play #1: Create an end-to-end consent and opt-out signaling system

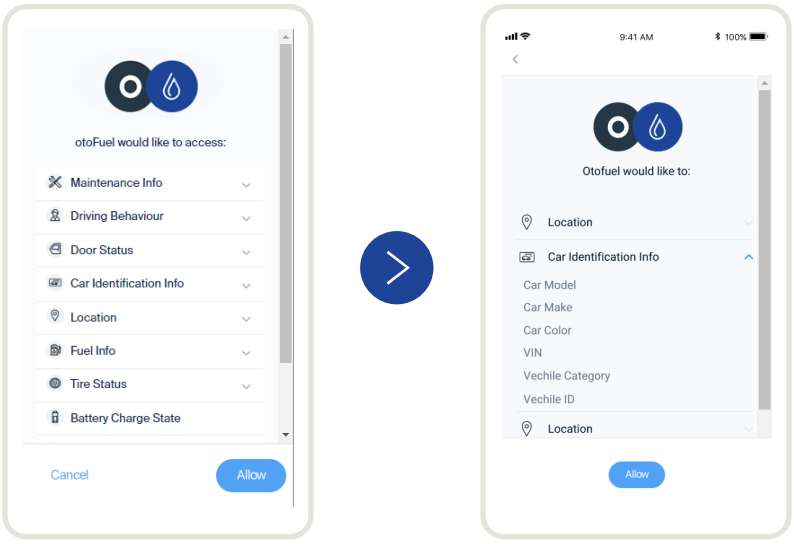
As the owners in most cases of the data pipe that collects connected car data, OEMs have the ultimate responsibility for informing their customers about connected car data collection and ensuring the appropriate permissions.[9] However, if consumers enter into an agreement with a third party for a service that depends on connected car data, they will be looking to that third party to inform them and to exercise their legal rights. The ideal customer experience would be an interconnected system that seamlessly transmits and records consent-related information across OEMs and the ecosystem of service providers using connected car data.

Establish trust via the entity with the direct consumer relationship

The best way to ensure a consumer is comfortable with data sharing is to provide the full context of how that data will be used. For example, if an insurance provider is collecting car data to gain accurate, real-time mileage data or a more comprehensive picture of a policyholder's driving behaviors, that insurance provider is probably in a better position to explain the value of its service and associated data flows than an OEM.

In this scenario, transparency about the collection of data would start in a service provider's app or website. The service provider would show the data parameters used in its service and capture the consumer's consent, which would then be transmitted to the OEM.

OEMs might also provide an interface in their mobile apps for services that they offer directly to their drivers or via partnerships with third parties.



Example of a consent management flow from a fueling app.

GDPR and the legal basis for collecting personal data

The European Union General Data Protection Regulation (GDPR) is a comprehensive regulation that governs personal data of EU persons and is expected to be supplemented by the ePrivacy Regulation in the future. The ePrivacy Regulation will enact requirements for a range of technologies including those used in vehicles. Japan, Brazil, South Korea, and other major jurisdictions have followed Europe in adding or updating data protection legislation. In the United States, California has led the way, and dozens of other states are following suit. U.S. federal legislation seems unlikely in 2019, but is likely to be enacted in upcoming years.

GDPR has set a precedent for data protection worldwide. It establishes six lawful grounds for collecting and processing various types of data:

1. **Consent:** The individual has given clear, affirmative consent for you to process their personal data for a specific purpose. Example: A driver chooses to share location and battery level in order to receive recommendations for nearby EV charging stations. Consent must be easy to revoke.
2. **Contract:** The processing is necessary for a contract you have with the individual, or because they asked you to take specific steps involving their data before entering into a contract. Example: An insurance provider needs odometer readings to administer a pay-as-you-drive insurance policy.
3. **Legal obligation:** The processing is necessary to comply with the law. Example: Many jurisdictions mandate the use of event data recorders that retain key safety information regarding automobile collisions.
4. **Vital interests:** The processing is necessary to protect someone's life. Example: Information may be used to identify which vehicles are the subject of a voluntary safety recall.
5. **Public task:** The processing is necessary for you to perform a task in the public interest or for an official function (and the task or function has a clear basis in law). Example: Traffic control managed by a municipality.
6. **Legitimate interest:** The processing is necessary for your legitimate interest of the controller or that of a third party. A balancing test must be conducted to ensure risks are assessed and safeguard implemented. Example: Statistics about wear and tear and performance are collected to improve a manufacturer's future models.

Validate consent with every data request

The interconnected system between OEMs and service providers needs to provide real-time insight into each consumer's consent status. The OEM essentially becomes an identity and access management provider, centralizing consent information for many service providers and authenticating each data request in real time.

Provide a control panel for data management and opt-out

Drivers should be able to see the data they're sharing and choose whether to turn off specific features or services at any time. Their choices should opt them out of related data collection. This modern user experience should be available through the OEM's website, mobile app, and infotainment system—not just buried within the privacy policy. This is clearly an area with room for improvement, since in a review of 12 OEMs' U.S. privacy policies, we found only two[10] that provided clear instructions on how to opt out of any data collection.

Although ownership of all consent management needs to rest with OEMs (the actual data collectors), consumers will often look to a service provider to revoke consent. Just as with opt-in, the OEM and the service provider need to provide a seamless experience to consumers that updates all systems behind the scenes, regardless of where a request was initiated.

Automate other data-related rights

Under various regulations, drivers may have the right to opt out of data sales (a requirement of CCPA), to access or download their data, or to have all of their data deleted (the "Right to be Forgotten" promulgated in GDPR and CCPA). Certain data must be made available in an easy-to-transfer method, under the right of portability in GDPR and CCPA. Today, the processes enabling drivers to exercise their rights tend to be manual.

> *When deciding whether to allow an app to collect data, the most important factors that drivers consider are how trustworthy they perceive the company to be (68% of drivers indicated this was 'very important'), and whether they are told exactly what the data are being used for and who has access to it (63% of drivers indicated this was 'very important').*
>
> Consumer Survey by Otonomo and Edison Research

Play #2: Offer choices even when it's not legally required

For the foreseeable future, it's inevitable that different jurisdictions will have different definitions of what constitutes "personal" car data and which data practices require driver consent. At a higher level, there are basic principles of fairness and meaningful choice that come into play.

Sharing certain types of car data will soon become a public good. For example, vehicle-to-vehicle communications could potentially eliminate many devastating car accidents. Governments may decide that there are certain situations where connected car data must be collected and shared with OEMs as well as public agencies and their service providers, such as smart city software. For example, participants in a workshop sponsored by the U.S. Federal Trade Commission suggested applying different sharing options depending on whether the data is safety-critical.[11]

There may be other situations in which OEMs offer drivers some choices about which third parties may use their aggregate data, similar to how Apple or Microsoft may ask you to share your crash data so they can improve their products. OEMs should clearly define different categories of aggregate data, for example de-identified location, speed, hard-braking events, road signs captured by in-car cameras, weather, or infotainment systems settings. They should explain the purposes of data collection and data sharing as well as the direct and indirect benefits to drivers. Drivers then have the context they need to make informed decisions about data sharing and gain a sense of control over how their data is being used.

> *"In a study conducted by the IBM Institute of Business Value, 62% of consumers said they would consider one auto brand over another if it had better security and privacy."*

Play #3: Deliver information in transparent, engaging ways

Writing a clear, easy-to-understand privacy policy is critical to maintaining consumer trust and is increasingly a legal obligation. The European Data Protection Board's Transparency guidelines,[12] advise of the need for concrete, definitive language and recommend avoiding the use of the words "may," "might," and "some." Our review of OEM policies shows room for improvement, as many companies continue to use vague terms like "may," often dozens of times in one policy.

Meeting legal requirements is an important goal, of course, but by improving customer engagement with a more dynamic approach, OEMs can foster driver trust and future-proof their regulatory compliance strategies.

Use plain language

Transparency starts with one simple change: Supplementing legalese with regular language. Ideally, the entire privacy policy could be written in plain language. If not, providing a summary or Frequently Asked Questions page would represent a big step forward for most OEMs.

Take a multi-channel approach

In addition, OEMs have a number of channels that they could employ for disclosure and education:

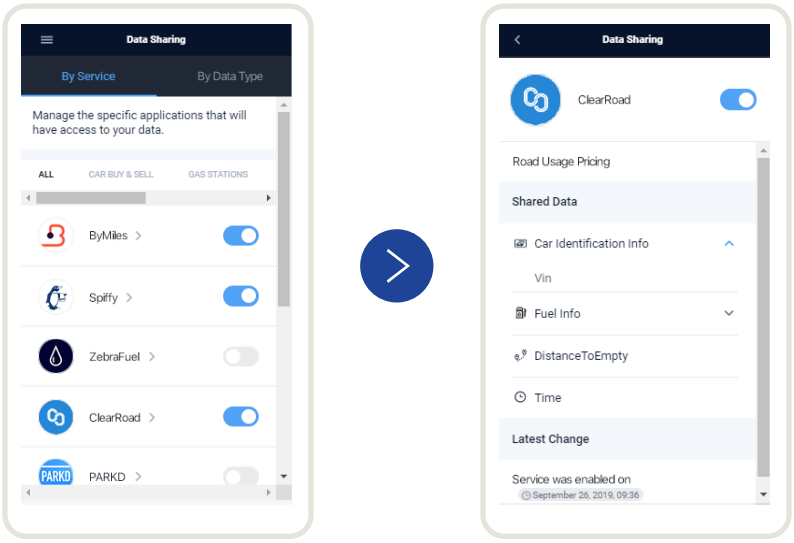
- Their websites, with an online hub for education and data management
- An online hub within their mobile apps
- The car's infotainment system
- In-person education at the dealership
- Videos that new car buyers can watch at the dealership or after purchase on the OEM's website
- A call center that can field privacy-related questions and inquiries, along with a 911-like capability for emergency response to potential car hacking

The challenge is to put these channels to work in a consistent way that creates a meaningful experience for consumers.

Education programs that take place in the dealership might include:

- One-on-one interactions with a sales representative
- A video for car buyers to watch while the dealer is detailing their car
- Paper handouts

OEMs may want to customize programs by car model, since each model may collect different data and provide benefits that appeal to different customer segments with unique information consumption habits. For example, younger buyers may care more about the congestion and pollution reduction benefits of sharing connected car data and prefer to watch a video. Consumers with families may care more about safety benefits and want paper handouts with links to a video they can watch at home.



Example of an OEM mobile app providing transparency about data sharing.

Provide visual indicators of data sharing and its impact

Another way to provide transparency is with a visual indicator on the infotainment system showing that the car is sharing data. This indicator could link to a "settings" feature in which drivers could see what data they are sharing, both personal and anonymous.

A Privacy Practices section on the infotainment center might also remind drivers of the indirect benefits of connected car data, such as reducing congestion, parking time, and pollution. OEMs with models targeting younger consumers might even incorporate gamification into their data-sharing disclosures, similar to Waze. For example, they could award points to people for miles and kilometers driven.

Play #4: Apply the minimal viable dataset to every situation

Connected cars have the potential to generate significantly more data than a single application or service needs. The best practice for each service is to only collect the minimal dataset needed to achieve its intended goals. For example, a roadside assistance app may need information about a vehicle's location, heading, and impact events, but not about its trip origination point or length. A subscription-based fueling app may need an unlock code for the car's gas cap but not for the car itself. A commercial fleet's incident-logging application for commercial fleets may receive eye-tracking data only when a hard-braking event is detected.

Play #5: De-identify data with context of the use case

Car data that has been legally de-identified, aggregated, and secured in a way that eliminates privacy risk to drivers is the holy grail. Everyone in the connected car data ecosystem seeks it, but achieving it is a constantly moving target. OEMs and service providers must always consider the fundamental challenge to anonymization: the mosaic effect. That is, de-identified data can become identifiable when combined with other public datasets. Every week there is a new research case showing how to re-identify some dataset.

Car data presents a unique barrier in that much of it is location based. Vehicle identification numbers (VINs), location data, car heading, or trip origination and termination points may all provide a view into consumers' private lives, depending on what other data is combined with it and how the information is processed. Blurring techniques are a potential solution. However, removing or blurring too much information also strips out value.

For each use of anonymized car data, developers and data analysts need to look at the essential data points they need and what can be blurred or redacted around those data points. For example, a parking app must have precise location accuracy to determine whether a parking space is available at a given point in time. However, it does not need to know whether the same vehicle is occupying that parking space, so any vehicle identifiers can be removed. An app that measures radio-listening habits, on the other hand, may need insight into listening time. It needs to know that data points coming in at a set interval

represent the same vehicle, but it does not need precise location, so GPS coordinates can be truncated to only include degrees of latitude and longitude.

It's important to view de-identification as a risk-mitigation tool. It can address technical challenges around using user-level or aggregate car data, but it does not eliminate all risk. OEMs and service providers will need to take a comprehensive approach that incorporates technical, contractual, and human processes.

Play #6: Secure car data from end to end

You cannot have privacy without security. Fortunately, automotive OEMs are taking data security very seriously. Heidi King, Deputy Administrator of the U.S. National Highway Traffic Safety Administration, said in a recent speech,[13] "Consumers need to trust that the sector is committed to working together to anticipate and mitigate cyber risks, and that the industry will react quickly and effectively when incidents occur. Trust is what we are building together as we step together into an increasingly digital future."

As connected car data and services play a larger role in the automotive ecosystem, the stakes are growing. As a case in point, 62% of respondents to a recent survey by Synopsis and SAE International[14] think that it's likely or very likely that malicious attacks on their software or components will occur within the next 12 months. No privacy playbook would be complete without a security play.

All participants in the connected car ecosystem need to invest in state-of-the-art infrastructure to protect car data. They need to apply both technical and organizational security measures as outlined in standards and best practices such as those from the U.S. National Highway Traffic Safety Administration,[15] the European Union Agency for Cybersecurity,[16] Auto-ISAC,[17] and the European Automobile Manufacturers Association (ACEA).[18] Furthermore, OEMs, service providers, and other stakeholders should continue to fund cybersecurity research and work together to create new cybersecurity standards that keep pace with industry changes.

> *"Sixty-four percent of respondents fear someone hacking into their connected cars and risking their personal safety."*
>
> Deloitte, 2019 Global Automotive Consumer Study

Biometric data: Raising the stakes

By Gail Gottehrer, Founder, Law Office of Gail Gottehrer LLC

As cars become more connected, more sensitive data is being collected. New vehicle services will include not just behavioral data such as hard braking or lane departures, but even more sensitive biometric data. Today, Cadillac and Volvo are both using eye tracking[19] to determine that a driver is attentive when cruise control is in use. Subaru has begun using facial recognition. In the startup realm, a number of companies are building solutions that purport to monitor drivers' health and even their emotional state[20] when they are in their vehicles.

The collection of biometric data significantly raises the stakes for privacy and security. Consumers can't change their fingerprints or irises like they change their passwords. Legislators are recognizing the importance of this data and are passing laws like the Illinois Biometric Information Privacy Act (BIPA), which requires written consent in order to collect biometrics data. The Illinois Supreme Court recently held that a claim for damages arising out of BIPA can proceed without any allegation of actual damage, concluding that the violation of the statute was enough to state a claim.[21] It's important to note that similar laws, and laws that define "personal information" or "private information" to include biometric data, are moving through the legislative processes in other states.

Play #7: Communicate broadly

Outside the automotive industry, media coverage of vehicle data tends to focus on surveillance and hacking, without considering the massive potential of connected car data for safety and convenience on the roads. The more participants in the connected car ecosystem work together to improve transparency and advocate the benefits of connected car data (e.g., improved safety, congestion, pollution, and convenience), the faster we can all earn consumers' trust. The Automotive Privacy Principles were a productive step for demonstrating privacy leadership in this sector, and companies should build on these principles to prioritize privacy in design and deployment of their systems.

The Future of Privacy Forum has partnered with the National Auto Dealer Alliance to publish a consumer guide, Personal Data in Your Car. This guide provides educational information to consumers in a non-promotional way.

Play #8: Think beyond a single vehicle owner or driver

Much of the discussion about connected car data privacy focuses on a single vehicle owner, who is also presumed to be the driver. However, there are many important situations to consider that break that simple model of data flows and consent.

Change of ownership

Connected car owners, and the car dealers who do business with them, must begin to adopt the same level of data hygiene for vehicles as we have become accustomed to with smartphones and computers. It will be imperative for entities operating in this space to facilitate the deletion of data between users, both on vehicles and in-vehicle apps.

Today, a vehicle's previous owner seems to be left with the responsibility of updating the OEM about a change of ownership. However, this process can leave serious gaps that could endanger users and owners.[22] For example, consumers have expressed concern that a previous owner's connected car app could unlock doors after a change in ownership.

We recommend that OEMs and their dealers take a leadership role on this issue. For example,

Volvo uses a third-party service that provides notifications when a Volvo is sold. In addition, there are machine learning solutions that can use connected car data itself (trips and location data points, for example) to detect possible changes in ownership. Armed with alerts, OEMs could reach out to their owners to determine if a car has changed hands.

Multiple drivers

Some applications may require different consent flows for different drivers. In particular, automakers should consider the implications of collecting data from a car that is driven by a consumer who is under the age of 18. As cars get more connected, it should be straightforward to create different driver profiles—with related consent flows—for different drivers.

Rental cars and car sharing

When a driver takes temporary ownership of a car through a rental car company or car sharing service, that car begins generating potentially identifying data about that driver. The data collected—about the driver, other vehicles, and the environment—is increasingly necessary for the vehicle to function. Today, there is no clear consent management process for rental cars or car sharing, and many anecdotal stories[23] about data being left for future renters to see. Data that remains on a vehicle can reveal sensitive personal information about consumers, including home addresses and location history.

Rental car companies contend that consumers should wipe their data before returning their cars, but this may be easier said than done.[24] The process is different depending on the make, model, and trim and involves multiple steps. And how many renters will be able to figure out the process?

First and foremost, rental car and car sharing customers should be given some meaningful choices about how their information is collected, processed, and used. They should be able to opt out—at minimum having the same types of choices they have with a vehicle they own. And they should be able to rely on the companies with which they do business to put in place appropriate data management, retention, and deletion policies and practices.

In addition, OEMs should consider adding a standardized "wipe" function to the infotainment system to facilitate clean transitions from renter to renter.

Ridesharing

Ridesharing is an interesting case for data collection consent and helps us to think beyond the car ownership model. Today, a ridesharing driver has a direct relationship to an OEM

and theoretically would be in control of data sharing. Tomorrow, autonomous ridesharing vehicles will be taking to the road, owned by ridesharing companies or by OEMs. (Elon Musk has tweeted that Tesla[25] could enter the ridesharing business in the future.) However, the car's location, heading, music being played on the car's sound system, and even ads or coupons that get displayed on the infotainment system are data points that are unique to the rider. In an ideal world, each rider would have easy-to-access privacy controls and some amount of control over what data they would share. The ridesharing app would then terminate consent automatically when the ride ends.

Play #9: Establish a data lifecycle strategy—including disposal

For every use case, there's a natural data lifecycle. Keeping data longer than necessary for business operations creates avoidable risk. Gail Gottehrer, Founder of the Law Office of Gail Gottehrer LLC, reminds us: "Storage is cheap, but risk is expensive!"

In addition to establishing strategies for collecting and storing data and managing consent, each participant in the connected car ecosystem should build comprehensive policies and procedures covering data retention and end-of-life data disposal that are based on actual business needs. This strategy should be in place even if all of the data you manage is de-identified and/or aggregated.

Companies can start the process of developing these policies and procedures by looking at:

- The practical, realistic useful life of data for each use case
- Any legal requirements that could mandate access to archived data (such as litigation holds or regulatory requirements)
- Practices for discarding raw, user-level data when your use case is based on aggregate data (and ensuring that any vendors or contractors who may have obtained the data from you during the process are legally obligated to discard the data, and in fact, do so)
- Automated data deletion according to your policies and procedures. You should also document the deletion process and keep that documentation with your business records, so that you have it in the event of regulator requests or litigation.

Get ready to put our plays into practice

By putting privacy at the center of your business practices, your company can accelerate the adoption of connected car data and the significant benefits promised by the new apps, services, and crowdsourced insights based on this new dataset. The game plan we have outlined in this playbook not only represents good consumer practices, but also aids in compliance with the plethora of laws and regulations that are in place and will continue to be enacted in many parts of the world. Regardless of whether your use case requires personal, vehicle-identifiable data or uses aggregate data, it's important to think about drivers' expectations and privacy concerns.

Fortunately, consumers place relatively high trust in automotive manufacturers. Seventy-two percent of drivers in the Otonomo-Edison survey—71% of new car buyers and 77% of connected car owners—were confident or somewhat confident that automotive OEMs would properly secure their data. The confidence measure for connected car owners compares favorably with that of credit card companies, with whom the vast majority of consumers have direct experience.

Building on their trusted consumer relationships, OEMs can develop a privacy-aware approach to connected car data and nurture a vibrant new ecosystem for their drivers. Doing so will be critical to their future success.

Acknowledgments

We'd like to thank Kelsey Finch, Jules Polonetsky, Lauren Smith, and John Verdi from the Future of Privacy Forum, Gail Gottehrer from the Law Office of Gail Gottehrer, Dan Or-Hof from the Or-Hof Technology and IP Law Office, and Todd Brockdorf, Petro Flomin, and Juergen Mayntz from Otonomo for their contributions to this white paper.

Endnotes

[1] Otonomo and Edison Research, "What American Drivers Think About Connected Car Data and Privacy," August 2018. Read Research >

[2] Deloitte, "2019 Global Automotive Consumer Study," January 2019. Read Study >

[3] For example, the state of Nevada recently passed a privacy law that allows citizens to opt out of the sale of their data by online service providers. The law specifically exempts automakers, repairers, and servicers from its requirements, but it is silent on whether it applies to a third party that receives data from an automaker.

[4] CCPA exempts ownership information retained or shared between a new car dealer and the vehicle's manufacturer from the right to opt out of vehicle information if the information is shared for the purpose of effectuating or in anticipation of effectuating a vehicle repair covered by a vehicle warranty or a recall, as specified. The law also exempts that personal information a business must maintain in order to fulfill the terms of a written warranty or product recall conducted in accordance with federal law from the right for a consumer to request that a business delete personal information about the consumer. "Vehicle information" is defined as the vehicle information number (VIN), make, model, year, and odometer reading. (Read the Read the California Legislature's Legislative Counsel Digest)

[5] Washington Post, "Alexa has been eavesdropping on you this whole time," May 2019. Read Article >

[6] Consumer Reports, "Samsung and LG smart TVs share your voice data behind the fine print," February 2015. Read Article >

[7] Axios, "Consumers kinda, sorta care about their data," February 2019. Read Article >

[8] Frost & Sullivan

[9] GDPR provides six lawful grounds for processing, of which contract, consent, legitimate interest, and contract performance are most often used depending on the nature of the service. See a more comprehesnive explanation from the Future of Privacy Forum on page 10.

[10] Nissan LEAF drivers get a dialog on their infotainment system that allows them to opt out of data collection. Tesla owners can send an email to Tesla to opt out of data collection.

[11] Federal Trade Commission and NHTSA, "Connected Cars Workshop: Federal Trade Commission Staff Perspective," June 2017. Read Study >

[12] European Comission, "Guidelines on Transparency under Regulation 2016/679," August 2018. Read Guidelines >

[13] NHTSA, "Auto-ISAC Cybersecurity 2018 Summit—In the Fast Lane," September 2018. Read Transcript >

[14] Ponemon Institute, "Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices," 2018. Read Study >

[15] NHTSA, "Cybersecurity Best Practices for Modern Vehicles," October 2016. Read Document >

[16] ENISA, "Good Practices for Security of Internet of Things in the context of Smart Manufacturing," November 2018. Read Document >

[17] AUTO-ISAC Summit

[18] ACEA, "ACEA Principles of Automobile Cybersecurity," October 2017. Read Document >

[19] Wired, "Cadillac's Self-Driving System May Be the Smartest Yet," June 2017. Read Article >

[20] Affectiva corporate website

[21] Illinois Official Reports, "Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Ill. 2019)," January 2019. Read Document >

[22] The Register, "Connected car data handover headache: There's no quick fix... and it's NOT just Land Rovers," August 2018. Read Article > The Verge, "Former VW owner discovered digital access to her car months after it was sold," May 2018. Read Article >

[23] Federal Trade Commission blog posts, "What is your phone telling your rental car?" August 2016. Read Article > "Leaving info behind, in (rental) cars," August 2016. Read Article > Privacy International, "Connected Cars: What Happens To Our Data On Rental Cars?" December 2017. Read Article >

[24] ZDnet, "Connected Cars: What Happens To Our Data On Rental Cars?" December 2017. Read Article >

[25] CNBC, "Elon Musk says self-driving tech could mean consumers will have a limited time to buy Teslas at current prices," July 2019. Read Article >

About Otonomo

The Otonomo Automotive Data Services Platform fuels an ecosystem of 15 OEMs and more than 100 service providers. Our neutral platform securely ingests more than 2 billion data points per day from over 18 million global connected vehicles, then reshapes and enriches it, to accelerate time to market for new services that delight drivers. Privacy by design is at the core of our platform, which enables GDPR and other privacy-regulation-compliant solutions using both personal and aggregate data. Use cases include emergency services, mapping, EV management, subscription-based fueling, parking, predictive maintenance, usage-based insurance, media measurement, in-vehicle package delivery, and dozens of smart city services. With an R&D center in Herzliya, Israel, and a presence in the United States, Europe, and Japan, Otonomo collaborated with twelve industries to transform their business with car data. More information is available at otonomo.io.

