



CONNECTED CARS AND THE THREAT TO YOUR PRIVACY

BY JUSTIN KLOCZKO



MARCH 2022

TABLE OF CONTENTS

Executive Summary	2
Introduction	5
Background	6
How Do Car Companies Acquire Your Geolocation Data?	8
What Do Companies Use Data For?	11
What Can Be Done About it?	21
Privacy Opposition	23

EXECUTIVE SUMMARY

Personal car data is the new gold rush of the auto industry. Cars collect more data than our phones.¹ As a result, car companies have become data miners.

Automakers have seized upon a data gold rush to monopolize our personal information for profit, including geolocation, according to an investigation by Consumer Watchdog.

Car companies, including General Motors, Toyota, Ford, reserve the right to collect, use and share data in order to track and market products. A car company like General Motors wants to be like Facebook.²

“Thirteen of the 16 selected automakers in GAO’s review offer connected vehicles, and those 13 reported collecting, using, and sharing data from connected vehicles, such as data on a car’s location and its operations,” said the United States Government Accountability Office.

And it is unclear at best if consumers own their data as car purchasing agreements are obscured in legalese. As a result, many sign their data rights away not knowing it, the investigation found. A *Harvard Journal of Law & Technology* study determined: “The current legal landscape suggests that all smart car data collected about the consumer, his location, driving behavior, and vehicle are all essentially owned by the smart car company.”³

California has new and old laws to combat the data mining around geolocation, which could stand as an important bulwark against tracking of drivers if properly implemented and protected.

The report’s key findings:

- The collection of car data is proliferating at an exponential pace. Over a span of only three months in 2021, for example, the number of companies that traffic in our personal data increased from 200 to over 500, according to Privacy4Cars.
- There is no such thing as “anonymized data.” Anonymized data, when paired with other data points such as credit card usage, can be used to identify you and target you, according to car technologists and privacy advocates interviewed by Consumer Watchdog.

¹ “Connected cars will send 25 gigabytes of data to the cloud every hour,” February 13, 2015: <https://qz.com/344466/connected-cars-will-send-25-gigabytes-of-data-to-the-cloud-every-hour/>

² “Vehicle Data Privacy,” United States Government Accountability Office, July 2017: <https://www.gao.gov/assets/gao-17-656.pdf>

³ “Who Owns the Data Generated By Your Smart Car?” *Harvard Journal of Law & Technology*, 2018: <https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech299.pdf>

- California Insurance Commissioner Ricardo Lara has recently started a [Twitter fight](#) with Elon Musk over using telematics data collected by cars in insurance rate setting, vowing to protect, “consumer data, privacy and fair rates.” Telematics is data collected and transmitted from a car. However, an investigation by Consumer Watchdog has found Lara is privately working with insurance companies on a proposal to allow electronic surveillance in California once he has the “political cover” to pull it off. According to a recording of a December meeting in Sacramento with Root Insurance, a telematics company, Root’s VP of Government Affairs said, “ Yes, so we have a lot of conversations with commissioner Lara in California. He is supportive of what we’re doing. He has asked us to go back and do a couple of things for him before he makes this move. He has asked us to, number one: build a coalition of partners so when he makes this move, he has support. If there is criticism he will have coalition of partners to say, ‘No, this is a good thing’....We’re building a coalition of partners in California, including the Hispanic Chamber of Commerce to have his back, give him the political cover when he makes this move. ..We’re grateful for his support and we’re working behind the scenes to provide everything we can as political cover for him.”⁴
- While location data can be turned off on your cellphone, there’s not yet an opt-out feature for your car.⁵ However, California is poised to be the first in the nation with an “opt-out” for precise geo-location that is set to take effect under the California Privacy Rights Act (CPRA) by 2023, when the newly-formed California Privacy Protection Agency issues rules in 2022 to allow for it under the CPRA – a ballot initiative passed by the voters in 2020 as Proposition 24.
- Companies are holding safety hostage to make consumers turn over their data. A car may ask if a driver would like to share his or her information with emergency responders. No one is going to say no to that. The problem is your information is not only being used for emergency response purposes, but for an array of other uses unrelated to safety.
- Car manufacturers are working with software companies to bring advertising right into the cockpit. Information from Chevy’s OnStar Service is directly fed to apps for Dominos, IHOP, and Shell, among others. Geolocation data customers include retailers like Starbucks, so they can better know when a person is likely to buy a cup of coffee.⁶ Once a car knows your data profile, your movements and your buying habits, the algorithm will steer you towards a buying frenzy. A scenario in which a

⁴ “Removing Bias in the Car Insurance Industry,” Root Insurance, Dec. 9. 2021, timestamp: 23:73, 34:28. <https://consumerwatchdog.org/sites/default/files/2022-03/RootZoom.mp4>

⁵ [“Your Car Knows When You Gain Weight,”](#) Bill Hanvey, *New York Times*, May 20, 2019.

⁶ [“Are car companies going to profit from your driving data?”](#) Sarwant Singh, *Forbes*, Nov 6, 2017. [“What does your car know about you? We hacked a Chevy to find out.”](#) Geoffrey A. Fowler, *Washington Post*, December 17, 2019.)

targeted coupon for McDonalds pops up on your infotainment system is not far away.

- Manufacturers have teamed up with data miners to geolocate cars in real time. Wejo, which touts its mobility data of over 10 million connected cars, claims to see the speed in which cars are traveling on 95 percent of U.S. roads. It has partnered with Palantir, the libertarian dream of Tech oligarch Peter Thiel, who has contracted with the military-industrial complex, including the LAPD, as well as the Department of Homeland Security, to help facilitate ICE raids. The U.S. Customs & Border Patrol has contracted out private data extraction firms for vehicle forensics kits, which disclose text messages, location, and pictures, down to which car door opened and at what time. All that has to happen is for your phone to pair with a car, or connected by USB. “When you plug it into this USB port, it’s going to charge your phone, absolutely. And as soon as it powers up, it’s going to start sucking all your data down into the car,” said Berla founder Ben LeMere, according to *The Intercept*.⁷
- One of the biggest misconceptions is that technology is making driving safer. It isn’t. The number of deaths per 100,000 miles driven grew in 2020 by almost 25 percent, according to the National Safety Council (NSC), marking the highest annual increase that the NSC has recorded in nearly 100 years.⁸ 2021 saw an increase in traffic fatalities, prompting the federal government to take action.⁹

A sea change in privacy is now happening. The California Privacy Rights Act will be implemented by 2023, a seminal law that enshrines consumers with new rights over a new subset of data deemed “sensitive personal information,” including geolocation. The law will allow consumers to “opt out” of their data being shared or sold, as well as requesting access to personal information collected, with the option to delete or modify it. But these proposed safeguards are being met with opposition by the insurance and automotive industry.

The Alliance for Automotive Innovation, which represents major auto manufacturers, is lobbying the California Privacy Commission to stop the opt-out¹⁰. The Personal Insurance Federation of California, a statewide trade association that represents seven of the largest insurers in America, is similarly lobbying for an exemption from the new law¹¹.

⁷ “Your car is spying on you, and a CBP contract shows the risks,” Sam Biddle, *The Intercept*, May 3, 2021: <https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/>

⁸ “Preliminary Semiannual Estimates,” National Safety Council, 2021: <https://injuryfacts.nsc.org/motor-vehicle/overview/preliminary-estimates/>

⁹ Buttigieg unveils a new strategy to combat rising car crash deaths, Hope Yen, *Los Angeles Times*, Jan. 27, 2022, https://www.latimes.com/world-nation/story/2022-01-27/buttigieg-vows-help-car-crash-deaths-spike?utm_source=pocket_mylist

¹⁰ Preliminary Written Rulemaking [Comments](#), pg. 125.

¹¹ [Preliminary Written Rulemaking Comments, pg. 131](#)

If the law is drawn correctly and the California Privacy Protection Agency(CPPA) listens to consumers and not special interest groups, the monopoly stranglehold over our personal data will be curbed.

INTRODUCTION

One of the largest industries in the world is the auto manufacturing industry.¹² By next year, 95 percent of new cars sold will be connected, meaning they will be essentially online computers on wheels.¹³ And personal car data is the new gold rush of the auto industry. Cars collect more data than our phones, often because they collect all of your phone's data on top of everything you do in the car. As a result, car companies have become data miners first and car manufacturers second. Tesla, for example, is a roving mass surveillance operation that collects information on not just you, but everyone you drive past. Teslas have up to nine cameras inside and outside the car.¹⁴

We have always feared Big Brother becoming reality. But the irony is we as citizens have become Big Brother, voluntarily recording, collecting and broadcasting everything for the world to see. We are both the ones doing the surveilling, and unwittingly let companies do it to us. The consequence is car companies basically reserve the right to do whatever they want with your data: to track, market products, and manipulate your insurance rates. A future where targeted ads pop up on your dashboard is not far off¹⁵.

The report will also highlight how California's seminal privacy initiative, the California Privacy Rights Act, gives consumers new rights regarding data protection. And it will spotlight the ways car manufacturers have monopolized consumer data and show how they are dangerous for privacy, with a focus on geolocation. What kind of data do car companies collect, and what they do with it?

Being able to shut off geolocation is elemental to consumer privacy. Pursuant to the California Privacy Rights Act, geolocation is considered "sensitive personal information." It is not necessary for the functioning of any car today. Car companies use and exploit precise geolocation data for future revenue streams, whether selling or sharing the data for profit, or future product development. The law requires that consumers have the opportunity to opt out of its use.

¹² Worldometers: <https://www.worldometers.info/cars/>

¹³ "Unlocking the full life-cycle value from connected-car data," McKinsey & Company, February 11, 2021: <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data>

¹⁴ "Consumer Reports says Tesla's cameras inside its cars, which transmit video footage of passengers, could pose privacy risk," Grace Kay, *Insider*, March 24, 2021: <https://www.businessinsider.com/tesla-in-car-cameras-pose-privacy-risk-consumer-reports-2021-3>

¹⁵ "Telenav launches connected in-car advertising platform for automotive OEMS," Telenav, January 4, 2018.

BACKGROUND

Car sales are historically lagging.¹⁶ Ford, for example, is selling less cars than it used to. So the car industry has to find ways to keep making money. That's where our personal data comes in. To manufacturers, it's an enormous pot of gold.

Our cars know more about us than we know about ourselves, information such as weight, blood pressure, sexual orientation, race, economic status, down to which doors open and what time you stepped on the brake¹⁷. They are vacuums that suck up reams and reams of data, much to our ignorance.

*“You’ve created
this connection
with merchants
and brands.*

*They know
your data.*

*We’re bringing
that onto the
dashboard of
the car.”*

“Your car knows you have a drug problem before anyone else does because you are in the wrong section of town at 3 a.m. where drug busts are occurring,” said Alastair Mactaggart, founder of Californians For Consumer Privacy, which spurred Proposition 24, the California Privacy Rights Act. “It knows when you’ve been fired.”

"Your driving behavior, the person in the car. We do have that data," said Rick Ruskin of General Motors. "You've created this connection with merchants and brands. They know your data. We're bringing that onto the dashboard of the car."¹⁸

Here's Ford CEO Jim Hackett in 2018 on the *Freakonomics* podcast.

“We know what people make. How do we know that? It's because they borrow money from us. And when you ask somebody what they make, we know where they work, you know; we know if they're married,” said Hackett. “We know how long they've lived in their house, because these are all on the credit applications. We've never ever been challenged on how we use that. And that's the leverage we got here with the data.”

And that information is used to directly advertise products, for corporate and governmental surveillance, as well as for insurance purposes. Many different entities will collect data from connected vehicles, “including car manufacturers, manufacturers of 'infotainment' systems,

¹⁶ U.S. car sales from 1951 to 2020: <https://www.statista.com/statistics/199974/us-car-sales-since-1951/>

¹⁷ [“Your Car Knows When You Gain Weight,”](#) Bill Hanvey, *New York Times*, May 20, 2019.

¹⁸ “Carmakers are collecting data and cashing in – and most drivers have no clue,” CBS, Nov. 13, 2018: <https://www.cbsnews.com/news/carmakers-are-collecting-your-data-and-selling-it/>



"Here's the screen that pops up every month. So far, I've always declined."

third parties that provide peripherals that plug into ports on cars, and auto insurance companies," according to the Federal Trade Commission.¹⁹

Although it seems bad now, we are only seeing the tip of the iceberg. For all the data monetization that is occurring, potential revenue streams are endless. By 2030, automotive data could become a \$400 billion industry, according to a 2021 report by global corporate consulting firm McKinsey & Co. Connected services are especially attractive because they provide high margins and recurring revenue streams. Cars with more features bring in four times the amount of revenue per car compared to a standard car. And it's been projected that cars will become more intelligent in the next decade, with improved sensors and cameras, enabling even more data points that can be sold.²⁰

¹⁹ Connected Cars, Federal Trade Commission, January 2018: https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf

²⁰ "Unlocking the full life-cycle value from connected-car data," McKinsey & Company, February 11, 2021: <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data>

While data is utilized in a number of ways to the consumer's advantage, such as locating a car after an accident or helping relieve traffic congestion, the financial incentive that comes from having such a massive trove of personal information is also a slippery slope. Tracking your location for emergency purposes doesn't mean manufacturers have the right to sell or share that information for something else. Many companies say their data is anonymized, meaning it's not attributable to a person's identity. But is it really anonymized?

"The reason why all of it is creepy is you cannot anonymize precise geolocation," said Andrea Amico, founder of Privacy4Cars, a company that seeks to delete personal data from cars. "I understand these are blue dots on a map. But imagine someone not knowing you, but still following you everywhere for 20 years? How do you not find that creepy?"

Further, anonymized data, when paired with other data points, can take on additional meaning, said a car technologist, whose identity we are protecting.

"The whole concept of anonymity doesn't mean the same thing it did a few years ago. What happens if they harmonize that info with credit card usage info nearby?" asked the technologist. "They can get around anonymization of that information by knowing who has been into a particular store; who is spending money there."

And maybe one of the biggest misconceptions is that the ubiquity of technology is making us safer. It isn't. The number of deaths per 100,000 miles driven grew in 2020 by almost 25 percent, according to the National Safety Council (NSC), marking the highest annual increase that the NSC has recorded in nearly 100 years.²¹

"Despite cars having more technology people are dying more often. Whatever we're doing with this data it isn't working," said Amico.

HOW DO CAR COMPANIES ACQUIRE YOUR GEOLOCATION DATA?

The top 16 automakers all collect our data, according to a study by the Government Accountability Office.²² While they state what kind of data is collected, whether it will be shared and for what purpose, most consumers don't know they allow companies to do this when they agree to purchasing a vehicle. These clauses are buried deep in agreements, lost in a jumble of fine print legalese. The study also found that none of the 13 car makers in the study that collected personal data had easy-to-understand privacy notices.

²¹ "Preliminary Semiannual Estimates," National Safety Council, 2021: <https://injuryfacts.nsc.org/motor-vehicle/overview/preliminary-estimates/>

²² "Vehicle Data Privacy," United States Government Accountability Office, July 2017: <https://www.gao.gov/assets/gao-17-656.pdf>

As long as a car has some version of connected services, such as an OnStar, it will collect data. According to Toyota's privacy policy, "If you do not deactivate Connected Services, you specifically consent to our electronic collection and use of your personal information and vehicle data and our storage of such data wherever we designate."²³

GM, for example, says, "The types of information may include but are not limited to." In other words, GM could collect any and all information it wants. The company says it will keep data "for as long as necessary."²⁴

Cars record geolocation every few minutes, some every few seconds. Companies acquire our location by lulling us in via the cloak of safety. A car may ask if a driver would like to share his or her information with emergency responders. "Who is going to say no to that?" asks Amico, the founder of Privacy4Cars. The problem is your information is not only being used for emergency respond purposes, but for an array of other uses unrelated to safety.

"They are holding safety hostage," he said.

Nissan vehicles will prompt drivers through its infotainment system by asking if you "consent to the transmission and use of your vehicle data." It's easy to say yes, but difficult to understand anything beyond that. The prompt merely says to see the owner's manual for more information.

Aside from cars recording your every move, people also unknowingly surrender their personal data by simply making an in-car call, connecting to Spotify, or even just charging their phone.

The founder of a Swedish data extraction firm Berla, which does business with car companies, as well as the United States government, bragged about the creepy ways in which it siphoned off people's personal information through a car's infotainment system:

"Your phone died, you're gonna get in the car, plug it in, and there's going to be this nice convenient USB port for you. When you plug it into this USB port, it's going to charge your phone, absolutely. And as soon as it powers up, it's going to start sucking all your data down into the car," said Berla founder Ben LeMere, according to *The Intercept*.²⁵

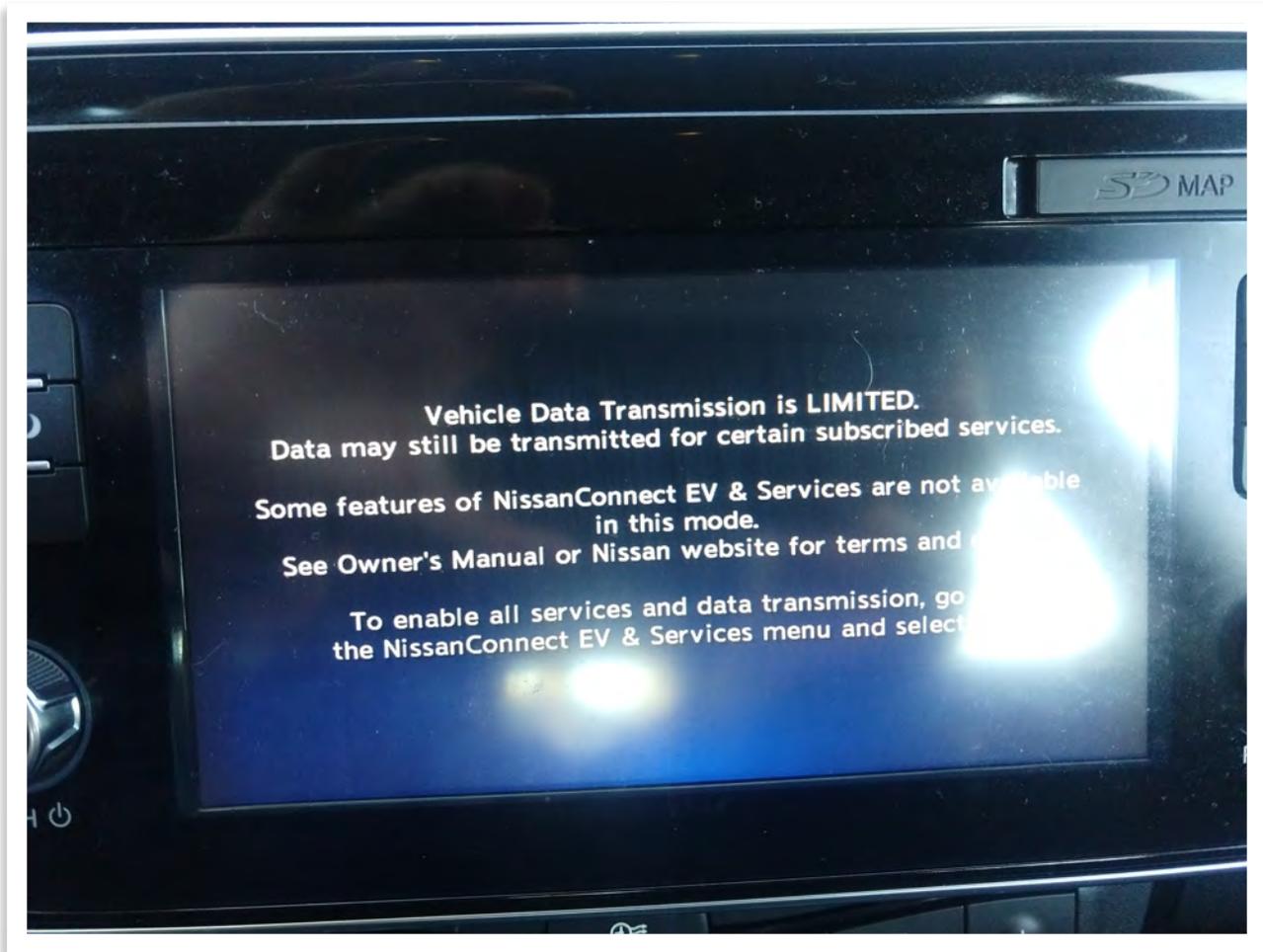
And there is usually more than one phone connected to a car.

"We had a Ford Explorer ... we pulled the system out, and we recovered 70 phones that had been connected to it. All of their call logs, their contacts and their SMS history, as well as their music preferences, songs that were on their device, and some of their

²³ Toyota privacy policy: <https://www.toyota.com/privacyvts/>

²⁴ General Motors privacy policy: <https://www.gm.com/consumer-privacy>

²⁵ "Your car is spying on you, and a CBP contract shows the risks," Sam Biddle, *The Intercept*, May 3, 2021: <https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/>



“This is with minimal connectivity selected. Model year 2018 Nissan.”

Facebook and Twitter things as well. ... And it’s quite comical when you sit back and read some of the text messages,” said LeMere.

A *Washington Post* investigation found that the Chevy’s dashboard didn’t disclose what it was recording. It wasn’t in the manual and there was no way to download it. So the reporter had to hire a hacker to literally dismantle the car. And what he found were phone logs, contacts, addresses, emails and photos.

“It contained enough data to reconstruct the Upstate New York travels and relationships of a total stranger. We know he or she frequently called someone listed as ‘Sweetie,’ whose photo we also have. We could see the exact Gulf station where they bought gas, the restaurant where they ate (called Taste China) and the unique identifiers for their Samsung Galaxy Note phones.”²⁶

²⁶ [“What does your car know about you? We hacked a Chevy to find out.”](#) Geoffrey A. Fowler, *Washington Post*, December 17, 2019.)

Multiple parties have their hands in the data pot as a result of different companies contracted out by manufacturers, according to Amico. For example, when you use a GPS navigation tool, not only does the car maker have access to the data, but so do companies that sell tools to dealerships. A company that provides a map would have access to it, as well as the company that provides the infotainment system, firmware, CAN bus, and traffic data.

“All devices talk to each other,” said Amico.

It’s how a company such as data miner Wejo acquires its information, by providing data-rich traffic analysis to auto manufacturers. Wejo has recently partnered with Palantir, which has contracted with the LAPD, as well as the government to help facilitate ICE raids. Otonomo, which also harvests car data and describes itself as “uniquely positioned at the heart of the automotive data ecosystem,” touts partnerships with 16 manufacturers. The company said its “commercial use cases” include smart cities, dealerships, financial and insurance firms.²⁷ And it said “thousands of organizations” have access to their data, which is 4.3 billion data points per day.

In addition, Aptiv, which provides technology for autonomous driving, among others services, says it shares personal data with third parties.²⁸

Further, you simply can’t stop cars from geolocating you.

Writing in the *New York Times*, the president of the Auto Care Association, said: “You may or may not choose to share your data with these services. But while you can turn off location data on your cellphone, there’s no opt-out feature for your car.”²⁹

WHAT DO COMPANIES USE DATA FOR?

To Sell You Things

Your information is sold by manufacturers to other connected car data companies such as Wejo, Otonomo or Palantir. Companies also get data from third-parties.

Consumer data gets into the hands of third-parties that don’t have any interest in helping enhance the driver experience. According to an investigation by the *Washington Post*, information from Chevy’s OnStar Service is directly fed to apps for Dominos, IHOP, and Shell, among others. Geolocation data customers include energy companies and retailers like

²⁷ Otonomo presentation: <https://www.documentcloud.org/documents/20515641-otonomo-presentation>

²⁸ Aptiv privacy statement: <https://www.aptiv.com/en/privacy-statement>

²⁹ “[Your Car Knows When You Gain Weight.](#)” Bill Hanvey, *New York Times*, May 20, 2019.

Starbucks and McDonalds, so they can better know when a person is likely to buy a cup of coffee or meal, according to Forbes.³⁰

Although we aren't quite there yet, the ubiquity of targeted advertising that has become the norm on our phones is coming to the driver's seat.

A likely scenario on the horizon is driving your family home when an ad pops up on your car's dashboard with a Pizza Hut coupon. A person would be able to voice-activate the order and pay for the meal through the car's infotainment system. Your car could also help you identify parking, or assist you in pre-paying for a meter. Everything will be done through your car.

"Or, if you're searching for an independent garage to take your car in for maintenance, your dealer could catch on and give you a call," according to the *Globe and Mail*.³¹

Our email inboxes and social media feeds are already filled with spam as a result of targeted advertising. Virtually our entire online experience is filled with it. If that is already the norm for our cellular devices, who is to say that won't happen with our cars?

One company in the process of making this a reality is Telenav, a software company developing in-car advertising software. It has followed the "freemium" model popularized by streaming services such as Hulu and Spotify, where in exchange for free services, consumers will be flashed with ads. Pop-up car ads could generate an average of \$30 annually per car.³²

Indeed, at the turn of the century, Telenav was the first company to integrate navigation and location-based services in mobile devices. Now it is advocating for advertising right in the dashboard.³³

In this auto surveillance-commerce world, the software company Telenav said there is a large opportunity to capitalize on the \$212 billion commuters spend while driving.³⁴

*"This is how we
ended up with
over 500
companies that
have your data.*

*Three months ago,
it was 200."*

³⁰ "[Are car companies going to profit from your driving data?](#)" Sarwant Singh, *Forbes*, Nov 6, 2017.

³¹ "What kind of data is my new car collecting about me? Nearly everything it can, apparently," Matt Bubbers, *The Globe and Mail*, January 15, 2020: <https://www.theglobeandmail.com/drive/technology/article-what-kind-of-data-is-my-new-car-collecting-about-me-nearly-everything/>

³² "[Pop-up ads in your car? It could be the next big thing.](#)" Gabrielle Coppola and David Welch, *Chicago Tribune*, March 6, 2018.

³³ "Why in-car advertising works," Telenav, June 14, 2018: <https://www.telenav.com/blog/why-in-car-advertising-works>

³⁴ "[Telenav advances in-car commerce, adds Alexa integration.](#)" Christie Schweinsberg, *Wards Auto*, Jan. 9, 2019.

These companies know that our car data is the key to unlocking our consuming behavior.

The *Globe and Mail* report goes on to say:

“That information may be used to collect outstanding debts, to target ads, to provide customer support, and to develop new products and services, among other things...That data can also be shared with third-party businesses, content providers, dealers, researchers, as well as law-enforcement agencies and the government, where required or permitted by law.”³⁵

Wejo touts its mobility data of over 10 million connected cars, which it says it can access in real time. It can even see the speed in which cars are traveling on 95 percent of roads in the U.S.

The Ulysses Group, a location-based intelligence company, said in its own documents: “Ulysses can provide our clients with the ability to remotely geolocate vehicles in nearly every country except for North Korea and Cuba on a near real time basis,” according to a company document. “Currently, we can access over 15 billion vehicle locations around the world every month,” the document adds³⁶.

“This is how we ended up with over 500 companies that have your data. Three months ago, it was 200,” said Amico, the Privacy4Cars founder.

Police State Surveillance

It’s not only rogue private companies who are using your geolocation and data, but governments as well. Together, they have harmonized massive amounts of data in the name of public safety and mass transportation. We know the U.S. Customs & Border Patrol paid private data extraction firm MSAB for hardware, including vehicle forensic kits manufactured by Berla, the company mentioned earlier that bragged about all the sensitive personal information it acquires.

CBP, which is a division of the Department of Homeland Security, believed the kit would be “critical in CBP investigations as it can provide evidence [not only] regarding the vehicle’s use, but also information obtained through mobile devices paired with the infotainment system.” According to the government contract, such a product was the only tool available for purchase that could tap into such systems.³⁷

³⁵ “What kind of data is my new car collecting about me? Nearly everything it can, apparently,” Matt Bubbers, *The Globe and Mail*, January 15, 2020: <https://www.theglobeandmail.com/drive/technology/article-what-kind-of-data-is-my-new-car-collecting-about-me-nearly-everything/>

³⁶ Ulysses Group: <https://www.documentcloud.org/documents/20515640-ulysses-document>

³⁷ “Your car is spying on you, and a CBP contract shows the risks,” Sam Biddle, *The Intercept*, May 3, 2021: <https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/>

The company touts access to cops: “Recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been.” This includes when car lights are turned on and which doors are opened at a specific time. It also advertises its ability to retrieve deleted data, divine “future plan[s],” and “Identify known associates and establish communication patterns between them.”

This poses a huge risk for constitutional protections against unreasonable searches.

We know surveillance contractors have been pitching and doing business with other branches of the federal government, saying they can geolocate cars in real time, according to reports from *The Intercept* and *Vice*.

The recent government infrastructure bill proposed tracking location data as part of a pilot program that would charge drivers’ per-mile travel fees.³⁸ The government said it would gather information about miles driven from smartphone apps, automakers, insurance companies, and gas stations.

“It’s concerning to see the advancement of a plan that appears to depend on the government’s mass surveillance of vehicles’ location simply to function,” Sean Vitka, policy counsel at Demand Progress, told *The Intercept*.

Insurance Telematics

The top ten automakers provide driving data, or telematics, to insurance companies to determine insurance rates. Everything from brake patterns, speed, to what time of day and where people drive, is collected.

“Liberty Mutual, for example, says it may gather data including mobile phone type, ignition status, vehicle diagnostics, and fuel consumption—even though that information doesn’t figure into a user’s premium pricing or discounts,” according to Consumer Reports.³⁹

Companies such as Ford said it would give owners cheaper insurance in exchange for their data, according to the *Wall Street Journal*.

But what are the implications for drivers? Some insurers’ algorithms are already misinterpreting metrics gathered through telematics as bad driving that, in fact, are not. For example, leading insurance companies such as Travelers, Allstate and Progressive have miscategorized what is considered “hard braking,” according to a 2021 *Consumer Reports*

³⁸ “Infrastructure bill could enable government to track drivers’ travel data,” Sara Sirota, *The Intercept*, August 5, 2021: <https://theintercept.com/2021/08/05/infrastructure-bill-travel-data-cars-privacy/>

³⁹ “What you’re giving up when you let your car insurer track you in exchange for discounts,” Kaveh Waddell, *Consumer Reports*, Oct. 7, 2021: <https://www.consumerreports.org/car-insurance/how-car-insurance-telematics-discounts-really-work-a1549580662/>

investigation. *Consumer Reports* said an 11 mile per hour decrease over a second was not considered “hard braking,” but according to these insurers, hard braking was considered to be between 6 and 10 mph within one second. Hard braking can also be a sign of an alert driver. The insurance companies are then using these incorrect assumptions to set rates.



“Vehicle data transmission is on!”

Companies also raise premiums for driving late at night or early in the morning. This disproportionately impacts minorities and working people who are more likely to work lower-paying third-shift jobs overnight.

Even tracking drivers’ speed could be misused. Imagine an accident where the insured is 1 or 2 miles over the speed limit. That data could be used against the “speeding” driver. And will those who opt out of data collection be penalized by having their premiums hiked up?

The number of auto-insurance policies in North America that use digitally-logged data from cars is projected to grow to nearly 50 million in 2023. That’s up from about 10.6 million in 2018, according to Berg Insight, a Sweden-based research firm.⁴⁰

A major claim of the insurance industry in favor of a data-driven model is that it will eliminate the discrimination inherent in current practices, including basing rates on ZIP Code or credit score, both factors that disproportionately harm lower-income drivers and communities of color. But telematics are likely to create a new set of discriminatory parameters and, with GPS tracking where drivers’ go, replace ZIP code with precise geolocation to enable ever more granular location-based redlining.

Consumers can’t even shop and compare premiums because each company uses different standards. How do we know that what is inside the car’s black box isn’t a new mechanism for discrimination? Or is it a way to discriminate against consumers who want their privacy protected? Can one really opt out?

⁴⁰ “Gm to sell car insurance, using data on your driving to set prices,” Mike Colias, *The Wall Street Journal*, Nov. 18, 2020: <https://www.wsj.com/articles/gm-wants-to-not-only-sell-cars-but-insure-them-too-11605708000#:~:text=The%20number%20of%20auto%2Dinsurance,a%20Sweden%2Dbased%20research%20firm>.

The Personal Insurance Federation of California, a statewide trade association that represents seven of the largest insurers in America, is lobbying the state of California regarding the CPRA rulemaking. It is against any limitations on collecting driver information and using it in setting rates.⁴¹

Speaking at a Consumer Federation of America panel in December 2021, a former insurance executive spoke on the complex algorithms telematics companies use.

“If you’re going to use an algorithm, you have to be able to explain it. Even data scientists don’t understand some of these algorithms,” said Sonja Larkin-Thorne, retired vice president of The Hartford, and chair of the State of Connecticut Insurance Department Advisory Council.

Tech companies masquerading as insurance purveyors are hoping to disrupt California’s Proposition 103, the longstanding regulation that brought much-needed reforms to California consumers. Under the law, insurance companies cannot use telematics data, with the exception of annual miles driven, to determine rates. California is one of the few remaining states in the country where insurers are not allowed to use data gathered by telematics to set insurance rates. Even so, companies seek such data and use it in other states.

California’s insurance commissioner, Ricardo Lara, speaking in a closed-door meeting with the insurance industry in 2019, raised eyebrows when he said turning over personal car data would be a good move.

“I honestly think that if someone is monitoring the way you’re braking or how you’re driving - you better believe that’s going to change your driving behavior and that’s something that can save lives,” said Lara.⁴²

Caught on hidden video tape, Lara promised a group of 200 insurance industry lawyers at the Western Regional General Counsel Conference, “I’m ready to get creative, just like all of you have been for so many years — and now you have somebody who’s receptive to that in the department.”

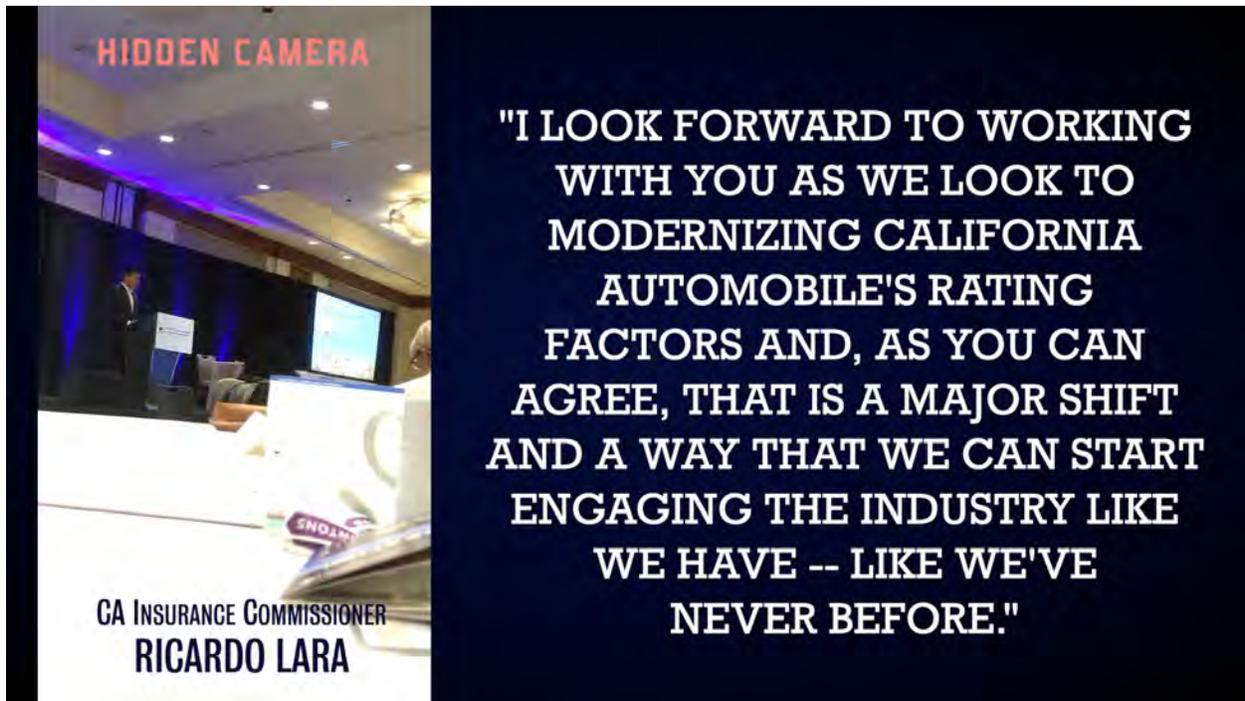
“I look forward to working with you as we work towards modernizing California’s automobile rating factors,” he said. “You can agree that is a major shift — and a way we can start engaging the industry like we have never before.”⁴³

Lara recently started a [Twitter fight](#) with Elon Musk over using telematics, vowing to protect “consumer data, privacy and fair rates.” However his comments at the general counsel conference, and other private conversations reported by the industry, suggest he is privately

⁴¹ [Preliminary Written Rulemaking Comments, pg. 131](#)

⁴² <https://www.consumerwatchdog.org/insurance/ricardo-lara-wants-give-insurance-companies-your-driving-data>

⁴³ <https://www.consumerwatchdog.org/news-story/lara-tells-insurers-hes-receptive-their-ideas-including-vehicle-data-use>



working with insurance companies on a proposal to allow electronic surveillance in California once he has the “political cover” to pull it off.

According to comments by telematics company Root Insurance, the company has been in discussion with Lara about incorporating consumer data such as speed and braking to determine insurance rates, which would infringe on privacy and only deepen premium discrimination.

“We have a lot of conversations with commissioner Lara in California,” said Root’s director of governmental affairs, Kathy Mitchell, during a December 2021 discussion sponsored by the California Hispanic Chambers of Commerce, captured on tape by Consumer Watchdog:

He is supportive of what we’re doing...He has asked us to go back and do a couple of things for him before he makes this move. He has asked us to, number one: build a coalition of partners so when he makes this move, he has support. We’re building a coalition of partners in California, including the Hispanic Chamber of Commerce to have his back, give him the political cover when he makes this move....We’re grateful for his support and we’re working behind the scenes to provide everything we can as political cover for him.

Root said it would seek to change Proposition 103 to include telematics driving data to determine insurance premiums.

Consumer advocates are concerned that telematics will only deepen existing discrimination by insurers.

AUTO INDUSTRY PRIORITIES:

By 2030, automotive data is projected to become a **\$400 billion** industry. Cars with more features bring in four times the amount of revenue per car compared to a standard car!

CONSUMER REALITIES:

The number of deaths per 100,000 miles driven grew in 2020 by almost **25 percent**, according to the National Safety Council (NSC), marking the *highest annual increase* that the NSC has recorded in nearly 100 years. 2021 saw an increase in traffic fatalities, prompting the federal government to take action.

In California everything an insurance company uses to set a driver's rate is public information. But insurance companies like Root tend to consider their telematics algorithm a trade secret. If Root's metrics for what is considered good or bad driving are a black box to consumers, we won't know what it is using to decide rates. California insurance companies are precluded from basing rates on ZIP-code, but if they know precise geolocation they can "redline" neighborhoods with far greater precision. If redlining is happening inside the black box of a telematics algorithm, we will never know it's happening.

The public would have no idea if insurers manipulated numbers inside a telematics black box. The black box model is already happening to some degree in the homeowners' insurance market in California, where insurance companies may use models to a limited extent to set fire insurance rates. Insurers, and in at least one case, the Department of Insurance, are actively blocking full disclosure of how the wildfire models use algorithms to assess fire risk.

Current Root customers complain about arbitrarily hiked rates, and also report the company's phone-based telematics app calculating their every move even when they are not driving, according to CNBC.⁴⁴

⁴⁴ A new kind of auto insurance technology can lead to lower premiums, but it tracks your every move," Mike Juang, CNBC, Oct. 6, 2018: <https://www.cnbc.com/2018/10/05/new-kind-of-auto-insurance-can-be-cheaper-but-tracks-your-every-move.html>

“The app begins crunching the numbers when: 1. I run on a treadmill 2. The airplane is taxiing before takeoff and after landing 3. I ride in an Uber / Lyft 4. I am in the passenger seat when my friend is driving,” [wrote a user named Venkat Raghavan](#).

Other common complaints include the app being unable to tell who is who.

“Not a very good system as it is fooled by others driving (you’re a passenger) and even walking up stairs. It tracks my wife and coworkers driving habits instead of mine,” said another user.

This highlights how our phones may not be accurate or reliable in collecting data in order to determine driving habits.

It is important to remember that Root is a self-described tech company masquerading as an insurance company. Data is gold to them. It collects it in a couple of ways. For those drivers who already have a connected car and are opted into data sharing, Root obtains that data from the car manufacturer, and uses that to formulate a price. For those that don’t have data, they must download Root’s app and complete a test drive for over a period of two to four weeks.

“Root's proprietary app collects their driving data using the sensors on their smartphone and transmits that data directly to Root for scoring,” a company spokesperson told Consumer Watchdog.

One issue with tech companies is everything becomes gamified. Root’s app is like a video game. But if you play stupid games, you win stupid prizes. Experience has shown that drivers will game the game.

Indeed, California consumers need a strong opt out mechanism for the use of precise geolocation to prevent insurance companies from illegally discriminating against them in underwriting and marketing based on the neighborhoods where they travel and live. For these consumers, it is a civil rights issue. California insurance companies are precluded from basing rates on ZIP-code, but if they know precise geolocation they can “redline” neighborhoods by not marketing to certain customers online.

California’s privacy commission can offer an opt-out provision for telematics tracking done by connected cars that would foil any new rule Insurance Commissioner Lara puts in place to allow car-based telematics. Unless Lara changes current rules, telematics will continue to be banned for auto insurance pricing in California.

This just the beginning of our private car data being monopolized.

“What can be mined—we are only hitting the tip of the iceberg,” said the car technologist. “We as people are dealing with massive amounts of data, and this is not something we have had to deal with in history before.”

Car rental data is a whole other racket. British Vehicle Rental & Leasing Association (BVRLA), a trade body for rental companies, said, “Collecting, analysing and delivering services based on this data will be a key revenue stream.”⁴⁵

And all it takes is to connect via Bluetooth onto a car’s infotainment system in order for it to download your contacts, texts, and phone calls. Each rental car sucks up tons of data because the average driver doesn’t delete their data before returning a vehicle. It’s up to the driver to delete the data, not the rental company. They hope you won’t.

And car companies know this. That’s why many policies reserve the right to keep your data indefinitely. They put such clauses in because they don’t know exactly what opportunities there will be to monetize the data —new revenue streams will emerge that aren’t currently apparent right now— so they broadly construe data ownership.

GM’s privacy statement says it will keep data “for as long as necessary.” Some insurance companies keep the data for 10 years. That’s longer than Google, which deletes location data after a year and a half.⁴⁶

Mactaggart, who spearheaded the California Privacy Rights Act, said: “Even if they haven’t figured out how to monetize it yet, they will. The data is so valuable.”

“Data fundamentally wants to be free and once you’ve generated information it is hard to get rid of it,” said the technologist. “It has a way of spreading from one place to another. Once it is out there it is very difficult to control all of it.”

⁴⁵ “Connected Cars: what happens to our data on rental cars?” *Privacy International*, Dec. 6, 2017: <https://privacyinternational.org/node/987>

⁴⁶ “What you’re giving up when you let your car insurer track you in exchange for discounts,” Kaveh Waddell, *Consumer Reports*, Oct. 7, 2021: <https://www.consumerreports.org/car-insurance/how-car-insurance-telematics-discounts-really-work-a1549580662/>

WHAT CAN BE DONE ABOUT IT?

Nearly 90 percent of surveyed consumers believe vehicle owners should control who can see their vehicle's data⁴⁷. The good news is that progress is being made, and the law is finally beginning to catch up with technology. In California, it's the passage of the California Privacy Rights Act (CPRA), a seminal piece of law that, with strong regulations, will bring much needed protections to consumers and their data. This is intended to be harmonized with the European privacy law. Under the CPRA, the California Privacy Protection Agency was entrusted with creating the rules and regulations to implement the law.

"We now have an agency—the first such privacy agency in the country—with dedicated funding, and a lot of it," said Mactaggart. "We're taking the lead here as the 5th largest economy in the world with good privacy regulations," he said.

A major component of the law, which will fully go into effect in 2023, enshrines consumers with new rights over a new subset of data deemed "sensitive personal information." The law will allow consumers to "opt out" of their data being shared or sold, as well as requesting access to personal information collected, with the option to delete or modify it.

"Sensitive personal information" includes precise geolocation, as well as Social Security numbers and driver's licenses; financial information such as credit or debit card numbers; religious or philosophical beliefs, union membership; race, ethnicity, email and text messages; genetic data; sexual orientation information, or health information. Under the CPRA, precise geolocation is defined as "data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations."

Additionally, the CPRA provides these new rights:

- If personal information held by a business, such as a car manufacturer, is inaccurate, consumers may request a correction.
- Consumers can opt out of automated decision-making technology, such as "profiling" related to decisions related to a person's movements, behavior, interests, health, economic information and work performance.
- Consumers can also access info about automated decision making.
- Consumers can limit the use and dissemination of sensitive personal information by businesses for "secondary" purposes, such as sharing with third parties, absent certain exemptions.

⁴⁷ ["Your Car Knows When You Gain Weight,"](#) Bill Hanvey, *New York Times*, May 20, 2019.

- Businesses must notify third parties who bought or received any consumer personal information to delete it. The agency has the discretion to provide a time period in which to take care of the violation.
- The opt-out right encompasses sharing of personal information for cross-context behavioral advertising. This is to regulate online advertising. The sharing of personal information for cross-context behavioral advertising can be opted out, but the use of personal information (save for geolocation) for non-personalized, first-party advertising is not.

Pursuant to the California Privacy Rights Act, geolocation is considered “sensitive personal information.” Regarding connected cars, being able to shut off geolocation is elemental to consumer privacy.

Car manufacturers are argue that there are “legitimate operational uses” for this data that should exempt them from the requirements of the law. The fact is there no legitimate operational use for sale or sharing of this data, or for the use of precise geolocation to the core functioning of the vehicle.

“Legitimate operational use” of precise geolocation data should be limited to any service a consumer has purchased or agreed to that requires precise geolocation data. For example, GPS maps have to track your precise location, but the sale or sharing of that data should be



subject to the “opt out” requirement because the sale and sharing of that data is not necessary for its operational use. Just because you agree to allow emergency response services to locate your car during an accident, does not mean companies can then share or sell that location data to McDonalds in order to help it decide when to try and sell you a Happy Meal.

“(CPRA) puts a magnifying glass on these companies,” said the technologist. But “it does not and cannot control accidental or malicious theft of data. Once that data gets out, I have to assume that anybody could get their hands on that data. And that’s the part that scares me.”

Exactly what “geolocation” will come to mean in the eyes of the CPRA will depend on the California Privacy Protection Agency (CPPA), the five-member board tasked with implementing and enforcing the law. It is currently undergoing a rule-making process, which has elicited responses from a range of industries.

PRIVACY OPPOSITION

A number of comments have been submitted to the CPPA regarding rule-making from a number of organizations. The voice of the automotive industry, the Alliance for Automotive Innovation, is lobbying the California Privacy Commission to limit the right to request correction of personal information that has been directly provided to the consumer. It has also come out against a global opt-out function for selling or sharing driver personal information⁴⁸. Under this proposal, consumers can’t correct information held by third-parties, or globally opt-out of the selling or sharing of their information.

“In almost all cases, an auto company does not know which consumer is using a particular vehicle at a particular point in time and would therefore not know when to honor a consumer’s opt-out preference,” stated the Alliance.

“As it is unclear how a global opt-out preference signal would work or translate effectively to the vehicle environment, it is premature for the agency to require that all businesses accept a global opt-out preference signal,” wrote the Alliance.

This reasoning is confusing because requesting an opt-out to one’s personal data has nothing to do with whether a company knows whose data is whose.

Privacy regulations will be adopted by the end of 2022 and will go into effect in 2023.

⁴⁸ Preliminary Written Rulemaking [Comments](#), pg. 125.