PRIVACY IN YOUR CAR: POLICY RECOMMENDATIONS FOR PROTECTING DRIVERS' DATA IN COMPREHENSIVE PRIVACY LEGISLATION

White paper by:

John Breyault
Vice President, Public Policy, Telecommunications, and Fraud

Colin Ganges
NCL Policy Intern

Brian Young
NCL Public Policy Manager

Sean Davis, Jr.
NCL Privacy and Technology Fellow

Pollyanna Turner-Ward
Google Public Policy Fellow

October 3, 2019
nclnet.org

"Nearly 90 percent of consumers believe vehicle owners should control who can see their vehicle's data. Currently they don't."[1]

New York Times, May 20, 2019

"Consumers should have the chance to delete their people search profiles whenever they want, and should be given access and deletion rights – or in some circumstances correction rights – with respect to the profiles that data brokers have about them."[2]

Former FTC Commissioner Julie Brill, April 15, 2015

"Cars not only know how much we weigh but also track how much weight we gain. They know how fast we drive, where we live, how many children we have — even financial information. Connect a phone to a car, and it knows who we call and who we text."[3]

New York Times, May 20, 2019

"A car can generate about 25 gigabytes of data every hour and as much as 4,000 gigabytes a day"[4]

Roll Call, April 9, 2019

"The Marketplace app is currently available in more than 2 million GM vehicles in the U.S. That number is expected to expand to 4 million by the year's end."[5]

Wall Street Journal, August 18, 2018

---

[1] Bill Hanvey. Your Car Knows When You Gain Weight. New York Times. https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html

[2] Evan Selinger. Why You Have the Right to Obscurity. https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0415/Why-you-have-the-right-to-obscurity

[3] Bill Hanvey. Your Car Knows When You Gain Weight. New York Times. https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html

[4] Roll Call. Your Car is Watching You. Who Owns the Data. https://www.rollcall.com/news/policy/cars-data-privacy

[5] Christina Rogers, What Your Car Knows About You: Auto Makers are figuring out how to monetize drivers' data. Wall Street Journal. https://www.wsj.com/articles/what-your-car-knows-about-you-1534564861

Executive Summary[6]

As the automotive and tech industries consider the deployment of autonomous vehicles, one of the pressing – yet often overlooked – issues is the privacy protections afforded to consumers. Vast amounts of data are collected by vehicle sensors such as engine control modules (ECM), event data recorders (EDR), and on-board diagnostic information (OBD-II) systems. These and other sensors collect data such as geolocation, speed, music choice, external information, in-cabin information, user recognition, app usage data and numerous other types of personal information. Vehicle owners may also choose to plug in a third-party device ("dongle") into their OBD-II to collect or share information about their vehicle with a third party of their choosing.

The list of in-car features and the data they utilize is evolving rapidly. Do consumers have a right to access or control the information collected from their use of automotive vehicles? Under U.S. law, drivers own data stored in event data recorders (EDR). However, no laws specifically address ownership of data collected by automakers through vehicle internet connections. This raises concerns because commitments made by automobile manufacturers[7] regarding data collection and use do not extend to third parties that may access data. Third party app providers often have their own policies about what data they gather and how they use it. We want to see that change.

This white paper reviews consumer rights and protections related to data collected by our vehicles. Polling finds that consumers, by overwhelming margins, believe that data collected by their vehicle is theirs to control and delete if they so choose. We therefore explore whether there is transparency about the collection and use of those data and whether consumers can control and delete what is being collected under various privacy regimes.

---

[6] For more information about this white paper, contact John Breyault, NCL Vice President, Public Policy, Telecommunications and Fraud at johnb@nclnet.org.

[7] Automotive Privacy Principles

While comprehensive privacy legislation is under Congressional consideration,[8] none of the bills introduced to date include language that specifically addresses data collected by automobiles from consumers. We agree with former Federal Trade Commission (FTC) Commissioner Julie Brill's recommendation to allow consumers to do all of the following:

- delete data;
- port data;
- obligate car manufacturers to secure consumer data; and
- give consumers information about what is being done with their data.

There are currently no limits on the amounts or types of data auto manufacturers can collect, nor are there any requirements for how auto manufacturers must safeguard their user's data. Likewise, there are no protections or notification requirements that could protect a consumer from having their sensitive data sold even though experts estimate that this data will be worth between $450 to $750 billion by 2030.

Data attributable to an individual is subject to the FTC's Fair Information Privacy Practices (FIPPs). Under the European Union's General Data Protection Regulations (GDPR), personal data is shared by manufacturers with third parties only on the basis of a contract with the consumer, prior consumer consent, and to comply with legal obligations.

[8] The DATA Privacy Act, S.583, https://www.congress.gov/bill/116th-congress/senate-bill/583/text?q=%7B%22search%22%3A%5B%22•%5CtThe+Digital+Accountability+and+Transparency+to+Advance+Privacy+Act%22%5D%7D&r=1&s=3
Data Accountability and Trust Act, H.R.1282, https://www.congress.gov/bill/116th-congress/house-bill/1282/text
Information Transparency & Personal Data Control Act, H.R.2013, https://www.congress.gov/bill/116th-congress/house-bill/2013?q=%7B%22search%22%3A%22The+Information+Transparency+and+Personal+Data+Control+Act%22%7D&r=1&s=1

NCL believes that any comprehensive federal privacy legislation must address automobile data collection. This should include the opportunity to control one's personal information, including, but not limited to: passwords, emails, contacts, locations, social security numbers, health records and entertainment preferences. In-car technology should provide consumers with options to understand what is being collected and easily delete information if they so choose. We also believe there must be a ban on contracts of adhesion (take or leave it contracts that if you don't agree to them, you can't access the service or good) and a ban on mandatory binding arbitration clauses. Data deletion options should be uniform across auto infotainment systems and enforceable by a private right of action.

The data collection protections NCL supports align with the protections the California Consumer Privacy Act (CCPA) affords California residents.[9] Auto owners, lessors and renters should have the right to:

- Know what personal information is being collected;
- Have the ability to access that information and share it with competing services;
- Know if their personal information is being disclosed and to whom;
- Know if their personal information is sold and to whom;
- Receive equal service and price whether or not they exercise their privacy rights;
- Not be forced to sign a contract of adhesion or to waive their rights to data protections as a condition of accessing the automobile service, whether in an ownership, rental or lease context; and
- Have a "data deletion" functionality built into the vehicle.[10]

Background

As the market share of so-called "connected" cars continues to rise, consumers have little choice but to purchase such vehicles. For example, General Motors was on track to double the number of connected cars installed with their Marketplace app from two million

[9] California Consumer Privacy Act of 2018, SB-1121, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121
[10] Id. at Your Car is Watching You. Who Owns the Data

to four million by the end of 2018. Other manufacturers have similar targets.[11] Sam Abuelsamid of Navigant Research notes that "we are not that far away from when 100 percent of all new cars will come equipped with data modems."[12]

Car manufacturers typically frame their near-total control of consumers' personal data via data ports and infotainment systems within connected cars as a convenience. Vehicle Generated Data (VGD) can be used by auto manufacturers to improve the driving experience, optimize products and services, increase driver comfort, and contribute to societal goals such as improving road safety and reducing fuel consumption. For instance, VGD may be used in the context of tire pressure, vehicle speed, mileage, fuel consumption, oil level, engine status, battery charge status, steering angle, and outside vehicle temperature.[13] There are many innovative applications as well, from real-time crash-prevention systems to anti-theft text alerts when a car is opened or activated.

Presently, car manufacturers are the near-exclusive keepers of much of the data cars produce.[14] Automakers use that information to point cars in need of repairs toward affiliated dealers.[15] Without regulation, companies have access to all VGD, providing them with insight into consumer's driving habits, such as speed, regular routes, phone calls, radio or telephone usage.

While there is a convenience to answering a phone call through a car, what privacy cost does such convenience entail? For example, such features can also allow car makers to collect personal information which they can – and do - sell to advertisers, insurance companies and other industries as they see fit.[16] California Senator Bill Monning introduced

[11] Christina Rogers, What Your Car Knows About You: Auto Makers are figuring out how to monetize drivers' data. Wall Street Journal. https://www.wsj.com/articles/what-your-car-knows-about-you-1534564861
[12] Michael Liedtke. Connected Cars accelerate down data-collection highway. Phys. https://phys.org/news/2018-12-cars-data-collection-highway.html
[13] Car Data Facts https://cardatafacts.eu/data-can-car-share/
[14] Jeremy B. White, Who Owns Vehicle-Generated Data? https://www.govtech.com/data/Who-Owns-Vehicle-Generated-Data.html
[15] Jeremy B. White, Who Owns Vehicle-Generated Data? https://www.govtech.com/data/Who-Owns-Vehicle-Generated-Data.html
[16] Id. at What Your Car Knows About You?

a bill to loosen car manufacturers' grip on VGD.[17] Monning's bill would allow consumers to see what data their car emits and decide with whom they want to share the information.

VGD can be attributable to specific individuals to varying degrees. Generally, VGD does not need such high protections as personally identifiable information (PII). However some types of VGD collection raise important privacy and data protection issues and are particularly sensitive. VGD that should be considered sensitive includes (but is not limited to) driver route, location data, and precise addresses visited. Data such as these must be protected to the same degree as PII.[18]

PII is any data that can be used to identify an individual. In the FTC's 2012 privacy report, the Commission stated that its privacy framework applies to "consumer data that can be reasonably linked to a specific consumer, computer, or other device."[19] However, the FTC also acknowledged that "the traditional distinction between PII and non-PII has blurred" and suggested that "it is appropriate to more comprehensively examine data to determine the data's privacy implications."[20] The National Institute for Standards and Technology defines PII as "any information about an individual, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[21]

---

[17] Senate Bill 994 California, Introduced by Senator Monning February 12, 2014
[18] https://dataconomy.com/2018/09/four-data-challenges-posed-by-the-connected-car/
[19] Federal Trade Commission, Protecting Consumer Privacy in An Era of Rapid Change: Recommendations for Businesses and Policymakers (2012) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
[20] Federal Trade Commission, Protecting Consumer Privacy in An Era of Rapid Change: Recommendations for Businesses and Policymakers (2012) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
[21] McAllister, E., Grance, T., & Scarfone, K. (2010, April). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (NIST Special Publication 800-122). Gaithersburg, MD: National Institute of Standards and Technology.

Car manufacturers collection of consumers' geolocation, destinations, phone numbers, call logs, and far more is not well understood by consumers. Tesla collects preferences on radio stations, frequent charging locations, and the condition of the car.[22] The *New York Times* reported that car companies know "how fast you drive, how hard you brake, whether you always use your seatbelt[.]" This information can be shared with insurance companies without consent.[23] More disturbingly, physical details, such as eye movements and the placement of hands on the steering wheel, may also be collected.[24] These data also come from smartphone connectivity which companies profit off of by various means, including creating targeted advertisements or by selling data to mapping apps.[25] [26]

Most consumers recognize how personal our cellphones are and that a data breach can compromise sensitive information. However, the connection between our phones and our cars is less understood. Automakers take advantage of that. In the lengthy fine print of auto sales agreements, car companies are explicit about their right to obtain consumers' most personal information. For example, a 30-page Tesla policy statement says "we collect three main types of information related to you or your use of our products and services: (1) information from or about you or your devices; (2) information from or about your Tesla vehicle; and (3) information from or about your Tesla energy products."[27] Tesla then says they have a right to collect "information from you or about you (such as you your name, address, phone number, e-mail, payment information, driver's license or other government identification information)."[28]

Collection of personal data by car companies is not a new phenomenon. However, the type and amount of information collected has grown exponentially as consumer data

[22] Joann Muller, What Tesla Knows About You. Axios. https://www.axios.com/what-tesla-knows-about-you-1f21d287-a204-4a6e-8b4a-0786b0afac45.html
[23] Id. at Your Car Knows When You Gain Weight
[24] Id.
[25] Id. at What Your Car Knows About You?
[26] Id. at Cars Suck Up Data About You. Where Does It All Go?
[27] Tesla. Consumer Privacy Policy. https://www.tesla.com/about/legal
[28] Id.

becomes more valuable. The data trove in the hands of car makers could be worth between $450 and $750 billion by 2030, according to the consulting firm McKinsey and Company.[29]

Digital advertising based on drivers' data has become a multi-billion-dollar business where consumers' privacy rights are at risk as the industry seeks to boost its profits. For example, Hyundai offers coupons for gas and other products to lure consumers into allowing their data to be collected and shared.[30] In Arizona, Farmers Insurance is offering customers a 3 percent discount just for using a smartphone app that tracks driving behavior, including whether the driver is holding a phone or using a hands-free Bluetooth connection.[31]

Privacy policies are often used by organizations to offer consumers choice in terms of how they use their data. However, privacy issues that arise in the context of automated vehicles make the consent model of privacy protection increasingly impractical. Rules are needed to establish privacy norms for organizations to follow regarding collection, use, and disclosure. [32]

Some automakers have agreed to allow consumers to opt-in to having their data shared before sharing certain details with third parties. However, absent robust privacy protections for consumer data, each company can decide what information to collect and what information does not require opt-in permission.[33] Opt-in or opt-out permissions do not automatically mean the data are accessible or deletable by consumers. When asked if automakers can currently be prevented from collecting our data, we learn that "most automakers let owners decline, or opt out of, data collection, but that's usually buried in the

[29] McKinsey & Company. Monetizing Car Data: New Service Business Opportunities to Create New Customer Benefits.https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx
[30] Id. at What Your Car Knows About You?
[31] Id. at Cars Suck Up Data About You. Where Does It All Go?
[32] Privacy, consent and vehicular ad hoc networks (VANETs) Rajen Akula. Computer Law & Security Review 24 (2018) 37-46
https://reader.elsevier.com/reader/sd/pii/S0267364917302170?token=A4FEA1A5E96CF874BCCAD18EF3D037A6EEAD94D08120654FB8B4C0AC58AFD598C95D0C281E43E4C19B41C21B41AAA253
[33] Id. at Connected Cars Accelerate Down Data-Collections Highway

fine print. Otherwise, permission is assumed."[34] Because of cumbersome and opaque opt-out policies, consumers continue to lose access to and control of their personal information.

The combination of increasing numbers of connected cars and complex opt-out procedures, along with a lack of consumer understanding of what is being collected also exposes consumers to data breaches when companies don't implement robust data protections. For example, Toyota this year announced that the company had suffered a security breach resulting in over 3 million Toyota and Lexus car owners' data being stolen.[35] This was the second major security breach for Toyota in a year.[36] Similarly, a Vietnamese hacking group known as APT32 successfully launched a spear phishing campaign (sending emails that appear to be from someone you know in order to gather personal information) against multiple car companies.[37]

Current Legal Protections Are Limited

None of the current federal privacy proposals before Congress specifically address consumer data collected by car companies. There is a patchwork of state and federal law which is not comprehensive. In 2018 California enacted the California Consumer Privacy Act (CCPA), which provides strong privacy protections. However, federal action by Congress has been at a standstill. American consumers currently have no universal right to see auto manufacturers' data collection policies or to know what information is being collected.[38]

[34] Id.
[35] Catalin Cimpanu. Toyota Announces Second Security Breach in The Last Five Weeks. ZDnet. https://www.zdnet.com/article/toyota-announces-second-security-breach-in-the-last-five-weeks/
[36] Eduard Kovacs. Millions of Toyota Customers in Japan Hit By Data Breach. Security Week. March 29, 2018 https://www.securityweek.com/millions-toyota-customers-japan-hit-data-breach
[37] Sean Lyngaas. Toyota Data Breach Affects Up To 3.1 Million Customers. Cyberscoop. https://www.cyberscoop.com/toyota-data-breach-japan-vietnam/
[38] Id. at Connected Cars Accelerate Down Data-Collections Highway

NCL strongly supports curbs on auto data collection that are specifically outlined in privacy legislation and which are focused directly on automakers collection of data manufacturers.

Below are some introduced bills which, with appropriate amendments could be viewed as frameworks to provide consumer control and protection from unlimited auto data collection:

- **18 U.S.C. § 2721**, The Drivers Privacy Protection Act of 1994 (DPPA). Passed as an amendment to the Violent Crime Control of Law Enforcement Act of 1994,[39] Congress passed the DPPA to prevent Department of Motor Vehicle (DMV) employees from illegally sharing civilians' data in connection with their motor vehicle record.[40] An amendment to the DPPA placed additional requirements on DMVs to obtain opt-in permission from consumers before their personal motor vehicle records can be sold or released to third-party advertisers.[41] The initial reason for the DPPA and the concern over unbridled access to consumer data was the discovery that an obsessed fan had hired an investigator to find an actress named Rebecca Shaeffer. The investigator found Shaeffer's address through her California motor vehicle records. The fan later stalked and murdered the actress. This tragic event compelled Congress to pass the DPPA and protect other drivers from becoming victims. Today, consumers are susceptible to the same privacy invasions but on a much larger scale.[42]

- **H.R. 3388, The Safely Ensuring Lives Future Development and Research in Vehicle Evolution Act (SELF DRIVE Act).** Introduced by Representative

[39] Cornell Legal Information Institute. 18 U.S. Code § 2721. Prohibition on Release and use of certain personal information from State motor vehicle records. https://www.law.cornell.edu/uscode/text/18/2721
[40]Epic. The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record. https://epic.org/privacy/drivers/
[41] Id. 18 U.S. Code § 2721
[42] Id. at Connected Cars Accelerate Down Data-Collection Highway

Robert Latta (R-OH) in July 2017,[43] the bill's passage in the House was prompted by a 2017 Federal Trade Commission (FTC) report that detailed the information car companies collected and highlighted that manufacturers of infotainment systems were sharing non-aggregate data, such as a car's geolocation, for emergency purposes.[44] The measure was aimed at manufacturers of highly automated vehicles to prompt them to develop cybersecurity plans and a process for controlling access to automated driving systems.[45] The report prompted the National Highway Traffic Safety Administration (NHTSA) to create voluntary federal guidelines for automated vehicles entitled Automated Driving Systems 2.0: A Vision for Safety.[46] However, these guidelines make no direct reference to privacy protections or protecting consumers' personal data and instead directed consumer issues to the FTC.[47] Without giving the FTC stronger privacy enforcement powers and increased staff to implement those enhanced powers, however, the Commission cannot adequately curb the misuse of data. Julie Brill, a former FTC Commissioner, acknowledged that "the laws that the FTC enforces are simply not strong enough to police today's complex digital economy". We agree with Commissioner Brill.[48]

- **H.R.1282, Data Accountability and Trust Act.** Introduced by Representative Bobby Rush (D-IL) in February 2019,[49] the bill would require entities that collect and preserve personal information about consumers to

[43] SELF DRIVE Act, H.R.3388, https://www.congress.gov/bill/115th-congress/house-bill/3388
[44] Connected Cars Workshop. Federal Communications Commission. https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf
[45] Id.
[46] National Highway Traffic Safety Administration. Automated Driving Systems 2.0 A Vision for Safety. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
[47] National Highway Traffic Safety Administration. Automated Driving Systems AV 3.0. https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems
[48] Julie Brill. Data Privacy: Consumers Want it, Businesses Need it- It's Time Our Government Delivers. The Hill. https://thehill.com/blogs/congress-blog/technology/445405-data-privacy-consumers-want-it-businesses-need-it-its-time-our
[49] Data Accountability and Trust Act, H.R.1282, https://www.congress.gov/bill/116th-congress/house-bill/1282

adopt specific policies and procedures to protect such information within one year of the bill's enactment. The measure would also authorize the FTC to issue regulations to more strongly enforce privacy protections for consumers.

- **H.R.2013, Information Transparency & Personal Data Control Act.** Introduced by Representative Suzan DelBene (D-WA) in April 2019,[50] the bill would require the FTC to regulate entities that collect sensitive information. Companies would have to provide consumers with opt-in permissions to collect, store, process, sell, or share sensitive information. It would also promote transparency about personal information by requiring that consumers not only know who has access to their information but know how to contact them. Finally, the bill would require a third-party audit of entities that control consumer information to evaluate whether a company's policies and practices are appropriate given the information collected.

- **Center for Democracy & Technology (CDT) Privacy Legislation Discussion Draft.** Released in December 2018,[51] CDT's privacy legislation discussion draft generally divides its provisions into two categories; "covered entities" (people or businesses that collect personal information) and "covered individuals" (United States citizens). Covered individuals are given five affirmative rights. These rights include a right to know, to portability, to access, to correct, and to delete. Covered entities on the other hand are given the responsibility to ensure redress, primarily by allowing consumers to make a complaint and that complaint to be responded to within a reasonable amount of time. The CDT draft also requires third parties to be held to the same standard as covered entities and states that covered entities may be

[50] Information Transparency & Personal Data Control Act, H.R.2013, https://www.congress.gov/bill/116th-congress/house-bill/2013
[51] Center for Democracy & Technology Discussion Draft, https://cdt.org/files/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf

required to act against a third party who does not comply with CDT's proposed standards.

- **S.2289, Data Breach Prevention and Compensation Act.** Introduced in July 2018 by Senator Elizabeth Warren (D-MA),[52] the bill would impose strict liability penalties at credit reporting agencies (CRAs). This would mandate a minimum penalty of $100 per consumer when a singular piece of personal information is stolen, and $50 for each additional piece of personal information. The penalty could not exceed 50% of the CRA's gross revenue. The bill would also require the FTC to allocate 50% of its penalty to compensate consumers. In cases where the CRA did not comply with the FTC's security standards or failed to report a breach, the penalty would increase to 75% of the CRA's gross revenue. The bill would also establish the Office of Cybersecurity at the FTC, which would supervise and provide annual cyber security inspections at CRA's.

- **Consumer Data Protection Act of 2018.** Introduced by Senator Ron Wyden (D-OR) in November 2018,[53] the bill would authorize the FTC to establish a minimum federal privacy and cyber security standard. When these standards are compromised and companies put consumers at risk, the FTC could issue a fine of up to 4% of the company's annual revenue and executives could face 10-20 years of criminal penalties. This level of oversight requires not only increased authority, but a larger protective force. This is why the bill calls for 175 new staff members to regulate the privacy market. Finally, the bill calls for increased transparency about what information consumers are providing to companies and the creation of a national Do Not Track system to ensure that third party companies cannot track them online.

[52] Data Breach Prevention and Compensation Act of 2018, S.2289, https://www.congress.gov/bill/115th-congress/senate-bill/2289
[53] Consumer Data Protection Act of 2018, Discussion Draft, https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf

- **S.3744, Data Care Act of 2018.** Introduced by Senator Brian Schatz (D-HI) in December 2018,[54] the bill would establish responsible duties such as the "duty of care," "duty of loyalty," and a "duty of confidentiality." Duties of care would be used to ensure that an online service provider secures consumer's personal information and discloses breaches of such data. The duty of loyalty would require that companies not use a consumer's data in any way that harms them, using the reasonable person standard. Finally, the duty of confidentiality would require that third parties abide by the same duty of care and duty of loyalty. If violated, the company would be subject to fines from the FTC, and civil enforcement actions from states.

- **S.583, The DATA Privacy Act.** Introduced by Senator Catherine Cortez Masto (D-NV) in February 2019,[55] the bill would require companies to identify information being collected and for what purpose, along with an explanation of who has access to the information. It would mandate that, where possible, data collected be deletable upon request by the consumer. Lastly, it outlines security standards to ensure that when personal information is collected, it is stored properly in order to minimize risk of data breaches.

Solutions

We believe Congress must address the collection of consumer information in keeping with consumer sentiment that is overwhelmingly supportive of maintaining greater control of their own data. This should include the ability to easily delete data on any vehicle a consumer owns, leases, or rents; establish mandatory opt-in permission for

[54] Data Car Act of 2018, S.3744, https://www.congress.gov/bill/115th-congress/senate-bill/3744
[55] DATA Privacy Act, S.583, https://www.congress.gov/bill/116th-congress/senate-bill/583

the collection, sharing, and use of sensitive data; and implement data usage minimization criteria for companies to follow.

Consumers must be able to delete data of their choosing, including sensitive and personal information about themselves, their friends, and their family. Car companies must not be left in sole control of such significant data gathering and usage. The option to delete also allows consumers to change their mind about what information they wish to share and makes sure that if car companies misuse their data, consumers can stop agreeing to its collection.

The right to delete data is fundamentally tied to the need for a mandatory opt-in permission. The converse, opt-out permissions, are too easily manipulated by placing them within large bodies of text, which makes the process of opting out unrealistic for most consumers. Consumers should also have the choice to provide data to a car company rather than the choice to rescind their presumed consent.

Finally, data minimization is an essential element to protecting consumers as it delineates a clear line between information which can be beneficial to a consumer's experience and the personal information that should be protected. Data minimization ensures that car companies use only as much information as they need and that the information collected is used for a specific purpose only. This makes clear that the consent given by the consumer is not a blanket permission to repurpose that data in whatever way the company chooses.

Congress should also reference and adopt recommendations from the 2012 FTC report entitled *Protecting Consumer Privacy in an Era of Rapid Change*.[56] The report calls for

[56] FTC. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

"making privacy the default setting for commercial data practices."[57] To achieve this goal, we agree with the FTC's recommendations to:

1. Build privacy into every stage of development;
2. Allow consumers to decide what data they wish to share, as well as the ability to enact a Do Not Track mechanism; and
3. Provide consumers with information on the collection and use of their data.[58]

Conclusion

NCL believes that consumer privacy is of paramount importance. This principle should apply to the car industry as it would to any other entity collecting consumers' data. Consumers believe they not only should control but are entitled to have control over the personal data they produce. How wrong they are in today's environment. Absent Congressional action, automobile manufacturers will continue to collect and use consumers' personal information as more "connected" cars are sold to consumers.

Congress must include language in federal privacy legislation that creates rules of the road for car companies' data collection practices and puts limits on their use of consumers' personal information.

Consumers believe they already have a right to control this information. Congress must legislate to ensure that they actually do.

[57] Id.
[58] Id.