

Date of Hearing: June 21, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Jesse Gabriel, Chair

SB 346 (Wieckowski) – As Amended June 15, 2022

SENATE VOTE: 36-3

SUBJECT: In-vehicle cameras

SUMMARY: This bill would require specified disclosures pertaining to the presence of an in-vehicle camera, as defined, in a motor vehicle upon sale or lease of a new motor vehicle; would prohibit the use of any image or video recording collected or retained through the operation of an in-vehicle camera for advertising, sale to a third party, sharing with a third party except as specified, retention at any location other than the vehicle itself without consent, or access by a person other than the registered owner of the vehicle without consent; and would prohibit a person from compelling a manufacturer or other entity to build specific features into an in-vehicle camera for surveillance purposes. Specifically, **this bill would:**

- 1) Require a manufacturer of a new motor vehicle model that is equipped standard with one or more in-vehicle cameras that is sold or leased in this state to disclose that fact in the owner's manual; and, for a vehicle equipped with an in-vehicle camera that does not come standard with the vehicle model, require the manufacturer to disclose that fact in a document sent to the seller or leaser of the vehicle.
- 2) Prohibit a person or entity from providing for the sale or lease of a new motor vehicle equipped with an in-vehicle camera in this state without prominently informing, during the purchase of the vehicle, as specified, either the user or the person designated by the user to purchase the vehicle.
- 3) Require the seller, prior to the execution of the conditional sales contract for a vehicle, to provide the user with a separate disclosure, either written or electronic, acknowledging the existence and operation of an in-vehicle camera in the purchased vehicle, and to obtain the written or electronic signature of the user or purchaser on that disclosure.
- 4) Specify that the disclosure pursuant to 3), above, shall be contained on a single document or single internet website that is separate from the conditional sales contract purchase order, and any other document; shall contain prescribed language, written in at least 20-point bold type, indicating the presence of an in-vehicle camera; and shall specify the rights and remedies available to the user pursuant to the bill.
- 5) Indemnify a person or entity from liability pursuant to a violation of 3), above, if the manufacturer of the vehicle is in violation of 1), above, with respect to that vehicle.
- 6) Prohibit the use of any image or video recording collected or retained through the operation of an in-vehicle camera for any of the following purposes:
 - Any advertising.
 - Sale to a third party.

- Sharing with a third party, unless either of the following apply: (a) the user has provided affirmative prior consent; the images and recordings are shared only to the extent necessary to either improve portions of a vehicle's safety system which rely on or utilize the in-vehicle camera or to diagnose, service, or repair the in-vehicle camera or vehicle equipment that relies on or utilizes the in-vehicle camera; recipients of the images or recordings do not use the images or recordings for any purpose other than the specified purpose, do not share or transmit the images or recordings, and do not retain the images or recordings longer than reasonably necessary to fulfill the purpose for which they were shared; and the user receives clear, meaningful notice prior to the sharing of the images or video recordings, including the party or parties with whom the images or recordings will be shared, and the purpose for which they will be shared; or (b) the images or video recordings are shared with a third party in order to comply with a valid verifiable consumer request pursuant to the California Consumer Privacy Act of 2018 (CCPA).
 - Retaining at any location other than the vehicle itself, unless the user has provided affirmative prior consent.
 - Download, retrieval, or other access by a person or entity other than the registered owner of the motor vehicle, unless the user has provided affirmative prior consent.
- 7) Require a person or entity that provides the operation of an in-vehicle camera in this state to provide effective mechanisms, without any cost, penalty, or unnecessary steps, for a consumer to revoke their consent provided pursuant to the bill's provisions after it is given, including at least one mechanism that utilizes the primary medium through which the person or entity communicates with users; and require such a person to honor the user's consent revocation, and delete from all locations other than the vehicle itself any image or recording associated with that user that has been collected, retained, downloaded, or retrieved by that person or entity, as soon as practicable, but not later than 30 days after the user revokes consent.
- 8) Prohibit a person or entity from discriminating against a user because the user has exercised any of their rights under the bill, including, but not limited to: denying goods, services, or benefits to the user; charging different prices or rates for goods or services, including through the use of discounts or other incentives or imposing penalties; providing a different level or quality of goods, services, or benefits to the user; suggesting that the user will receive a different price, rate, or level or quality of goods, services, or benefits; or considering the user's exercise of rights under the bill as a basis for suspicion of criminal wrongdoing or unlawful conduct.
- 9) Provide that images or video recordings retained through the operation of an in-vehicle camera may be retrieved or shared without the user's permission if any of the following apply:
- A court or other judicial or administrative authority having jurisdiction authorizes the retrieval of the images or video recordings and the video recordings are subject to the standards for admission into evidence required by that court or other administrative authority.

- The images or video recordings are retrieved pursuant to an investigation or inspection authorized by federal law to be conducted by the National Transportation Safety Board or the Secretary of Transportation, and the personal information of an owner or a lessee of the vehicle, including the vehicle identification number, is not disclosed in connection with the video recordings retrieved.
 - The images or video recordings are retrieved for the purpose of immediately determining the need for, or facilitating, emergency medical response to a motor vehicle crash.
- 10) Prohibit a person or entity from compelling a manufacturer or other entity providing the operation of an in-vehicle camera to build specific features for the purpose of allowing an investigative or law enforcement officer to monitor communications through that feature.
 - 11) Provide that actions for relief pursuant to the provisions of the bill may be prosecuted exclusively in a court of competent jurisdiction in a civil action brought in the name of the people of the State of California by the Attorney General or by any district attorney.
 - 12) Provide that a court may enjoin a person who knowingly engages, or has engaged, or proposes to engage in a violation of the bill's provisions; and may make any orders or judgements as may be necessary to prevent a violation of the bill's provisions.
 - 13) Provides that a person who knowingly engages, has engaged, or proposes to engage in a violation of the bill's provisions shall be liable for a civil penalty not to exceed \$2,500 for each vehicle equipped with an in-vehicle camera sold or leased in violation of the bill.
 - 14) Define, for the purposes of the bill, the following terms: "affirmative prior consent," "in-vehicle camera," "personal information," and "user."
 - 15) Specify that any waiver of the provisions of the bill is contrary to public policy and void and unenforceable.
 - 16) Specify that the remedies or penalties provided by the bill are cumulative to each other and to the remedies or penalties available under all other laws of the state.
 - 17) Specify that the provisions of the bill are severable, and that if any provision of the bill or its application is held to be invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

EXISTING LAW:

- 1) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (Cal. Const., art., Sec. 1.)
- 2) Provides that a plaintiff alleging an invasion of privacy in violation of the state constitutional right to privacy must establish each of the following: (1) a legally-protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant that constitutes a serious invasion of privacy. (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 40.)

- 3) Provides that there is a legitimate expectation of privacy in the interior of a car. (*People v. Bell* (1996) 43 Cal.App.4th 754, 770.)
- 4) Requires a manufacturer of a new motor vehicle sold or leased in this state that is equipped with one or more “event data recorders (EDR) or “sensing and diagnostic modules (SDM),” to disclose that fact in the owner’s manual for the vehicle. (Veh. Code Sec. 9951(a).)
- 5) Provides that specified data recorded on a recording device subject to 2), above, may not be downloaded or otherwise retrieved by a person other than the registered owner of the motor vehicle, except under specified circumstances, and prohibits any person authorized to download or otherwise retrieve data from a recording device pursuant to one of those specified circumstances from releasing that data, except to specified parties and only if the identity of the registered owner or driver is not disclosed. Specified data includes: 1) how fast and in which direction the motor vehicle is traveling; 2) a history of where the motor vehicle travels; 3) steering performance; 4) brake performance, including but not limited to, whether brakes were applied before an accident; 5) the driver’s seatbelt status; and 6) information concerning an accident that can be transmitted to a central communications system. (Veh. Code Sec. 9951(b)-(d).)
- 6) Prohibits a person or entity in the business of renting passenger vehicles to the public of using, accessing, or obtaining any information relating to the renter’s use of the rental vehicle that was obtained using electronic surveillance technology, except under specified circumstances. (Civ. Code Sec. 1939.23(a).)
- 7) Prohibits, with exceptions, electronic eavesdropping or recording of private communications by telephone, radio telephone, cellular radio telephone, cable or any other device or in any other manner. Violation can result in penalties of up to \$10,000 and imprisonment in county jail or state prison for up to one year. (Pen. Code Secs. 630-638.)
- 8) Prohibits cable and satellite television operators from monitoring or recording conversations in a subscriber’s residence, except as specified, or from sharing individually identifiable information on subscriber viewing habits or other personal information without written consent. (Pen. Code Sec. 637.5.)
- 9) Governs connected televisions, as defined, to prohibit any person or entity from providing the operation of a voice recognition feature within this state without prominently informing, during the initial setup or installation of a connected television, either the user or the person designated by the user to perform the initial setup or installation of the connected television. (Bus. & Prof. Code Sec. 22948.20(a).)
- 10) Prohibits actual recordings of spoken word collected through the operation of a voice recognition feature by the manufacturer of a connected television, or by a third party contracting with a manufacturer, for the purpose of improving the voice recognition feature, including, but not limited to, the operation of an accessible user interface for people with disabilities, from being sold or used for any advertising purpose. (Bus. & Prof. Code Sec. 22948.20(b).)
- 11) Prohibits any person or entity from compelling a manufacturer or other entity providing the operation of a voice recognition feature to build specific features for the purpose of allowing

an investigative or law enforcement officer to monitor communications through that feature. (Bus. & Prof. Code Sec. 22948.20(c).)

- 12) Establishes the CCPA to provide various rights to consumers. Subject to various general exemptions, the CCPA grants a consumer, among other things: (1) the right to know what PI is collected and sold about them; (2) the right to request access to the specific PI the business has retained about them; (3) the right to request the deletion of the PI that the business has collected about them; (4) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age; and (5) the right to pursue a cause of action against a business that has suffered a data breach in the event the consumer's PI has been impermissibly accessed. (Civ. Code Sec. 1798.100 et seq.)
- 13) Prohibits a business from discriminating against a consumer because the consumer exercised any rights under the CCPA, including, but not limited to, by: denying goods or services to the consumer; charging different prices or rates for goods or services; providing a different level or quality of goods or services to the consumer; or suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. (Civ. Code Sec. 1798.125(a)(1).)

FISCAL EFFECT: According to the Senate Appropriations Committee, “ongoing annual costs [to the Department of Justice] of \$366,000 for 1.0 Deputy Attorney General and 1.0 Legal Secretary to handle the anticipated workload associated with this measure, [and] unknown, potentially-significant workload cost pressures to the courts to adjudicate alleged violations of this measure.”

COMMENTS:

- 1) **Purpose of the bill:** This bill seeks to protect the privacy of drivers by ensuring that consumers are informed of the presence of in-vehicle cameras upon purchase or lease of a new motor vehicle and by providing drivers with additional control over the retention, use, and disclosure of data collected by in-vehicle cameras. This bill is sponsored by the Consumer Federation of California.
- 2) **Author's statement:** According to the author:

Drivers have a reasonable expectation of privacy in their vehicle that supersedes commercial interests. However, the use of in-vehicle cameras capable of generating valuable data threatens to erode such consumer privacy. Firms like BMW and General Motors already use inward facing video to monitor driver's attentiveness and gaze. Critically, the use of in-vehicle cameras will only grow. A report by Research and Markets estimates that the global automotive camera market will grow annually by 17.5%, reaching \$ 13.83 billion by 2026. Future software may also generate highly sensitive and valuable biometric data from these videos, i.e. the drivers' emotional state.

As stated, in-vehicle video is highly valuable. Vehicle-related data can be used [by] data brokers and firms to generate sophisticated composites of individuals for targeted advertisement. According to Mickinsey & Co., such vehicle-related data could be valued at \$750 Billion by 2030. This has incentivized firms like Amazon and Intel to build partnerships with automobile manufactures and gain access to their data. Although automobile firms have been reticent to share their data with third parties, a lack of

regulations means that the decision to share or not share data is left solely to the discretion of automobile firms. For example, in 2011 General Motors temporarily amended its terms and conditions for its OnStar system so that it could share vehicle information with third parties without explicit consent.

SB 346 would require customers to be informed, at the time of purchase, if a camera is installed inside a car, and would prohibit video recordings made of the interior of a car, by an in-vehicle camera, from being used for advertising or sold to third parties. Furthermore, this bill would prohibit manufacturers from retaining video recordings in any location, other than the vehicle itself, unless the user first provides affirmative written or electronic consent. It would also prohibit any person or entity from compelling the manufacturer, or entity providing the operation of an in-vehicle camera, to build features for the purpose of allowing an investigative or law enforcement officer to monitor communications through that feature. This bill would bring parity to the law by restricting the sale of private information collected by devices in consumers' private lives.

- 3) In-vehicle cameras and the reasonable expectation of privacy:** In 1967, the United States Supreme Court held that private conversations secluded from the public are protected against government surveillance under the Fourth Amendment's protections against unreasonable search and seizure. (*Katz v. United States* (1967) 389 U.S. 347.) The decision in that case relied heavily on affirming the existence of a reasonable societal expectation that private conversations in areas secluded from the public will be afforded privacy. Since then, the proliferation of so-called "smart" devices and vehicles, with the ability to both actively and passively collect various types of information, have redefined our understanding of this expectation.

The United States and California Supreme Courts have, on several occasions, affirmed that individuals possess a reasonable expectation of privacy inside their vehicles. (*See, e.g., United States v. Jones* (2012) 132 S. Ct. 945; *People v. Xinos* (2011) 192 Cal. App. 4th 637; *People v. Bell* (1996) 43. Cal. App. 4th 754.) This Legislature has also previously recognized the particular need to regulate surveillance in vehicles. In 2003, the Governor signed into law AB 213 (Leslie, Ch. 427, Stats. 2003), which required motor vehicle manufacturers to disclose in the vehicle's owner's manual if a vehicle sold or leased in this state is equipped with one or more "event data recorders (EDRs)" or "sensing and diagnostic modules (SDMs)," recording devices that collect certain telematics from the operation of the vehicle. AB 213 also prohibited any person other than the owner of a vehicle from downloading or otherwise retrieving EDR or SDM data, except with the consent of the owner or under specified circumstances. In 2004, the Governor signed into law AB 2840 (Corbett, Ch. 317, Stats. 2004), which prohibited a rental car company from using, accessing, or obtaining any information relating to a renter's use of the vehicle that was obtained using "electronic surveillance technology," except under specified circumstances.

This bill responds to the growing ubiquity of sophisticated in-vehicle cameras. In-vehicle cameras can serve a variety of functions, ranging from using facial-recognition technology to automatically adjust seat and mirror settings for each driver to detecting drowsy or distracted drivers and either alerting them or capping speed. In the United States, all new cars are required to have backup cameras to help drivers avoid accidents, and other countries have already expanded such safety requirements to include in-vehicle, driver-directed sensors and

cameras. However, little is known about how data collected by these cameras are stored and used, and with most new cars sold in the United States, including all new Fords, GMs, and BMWs, and nearly all Toyotas and Volkswagens, coming with built-in internet connections, the possibility that such private data is being made immediately accessible to automobile manufacturers without the knowledge or consent of the driver arguably warrants specific protections.

Recognizing the privacy implications of advances in technology equipped to motor vehicles, this Legislature has on several occasions placed limitations on the collection or use of certain vehicle diagnostic and surveillance data. AB 213 (Leslie, Ch. 427, Stats. 2003) responded to the growing number of vehicle manufacturers “installing recording devices in vehicles that may perform a variety of functions, from recording and transmitting accident data to recording a history of where the vehicle travels,” and provides that a manufacturer of a new motor vehicle sold or leased in this state that is equipped with an “event data recorder (EDR)” or “sensing and diagnostic module (SDM)” shall disclose that fact in the owner’s manual, and may not download or otherwise retrieve any of the following data except under specified circumstances: recordings of how fast and in which direction the motor vehicle is traveling; recordings containing a history of where the motor vehicle travels; recordings of steering performance; recordings of brake performance, including, but not limited to, whether brakes were applied before an accident; recordings of the driver’s seatbelt status; or information concerning an accident in which the motor vehicle has been involved.

Circumstances in which such data can be downloaded or otherwise retrieved by a person other than the registered owner of the motor vehicle are limited to the following: 1) the registered owner of the motor vehicle consents to the retrieval of the information; 2) in response to a court order; 3) for the purpose of improving motor vehicle safety, provided the identity of the registered owner or driver is not disclosed in connection with the retrieved data; or 4) the data is retrieved by a licensed new motor vehicle dealer or automotive technician for the purpose of diagnosing, servicing, or repairing the motor vehicle. In any one of these permitted circumstances, a person authorized to download or otherwise retrieve this data may not release that data, except to share among the motor vehicle safety and medical research communities to advance motor vehicle safety, and only if the identity of the registered owner or driver is not disclosed.

AB 2840 (Corbett, Ch. 317, Stats. 2004), established specific limitations governing the use of electronic surveillance technology by persons or entities in the business of renting passenger vehicles to the public. Specifically, AB 2840 prohibits a rental company from using, accessing, or obtaining any information relating to the renter’s use of the rental vehicle that was obtained using electronic surveillance technology, except under specified circumstances. For the purposes of that chapter, “electronic surveillance technology” is defined to mean a technological method or system used to observe, monitor, or collect information, including telematics, GPS, wireless technology, or location-based technologies, but *not* including EDRs, SDMs, or other systems used for the purpose of identifying, diagnosing, or monitoring functions related to the potential need to repair, service, or perform maintenance on the rental vehicle, or as part of the vehicle’s airbag sensing and diagnostic system. Specified circumstances in which electronic surveillance technology can be used are limited to locating a stolen, abandoned, or missing rental vehicle if it has not been returned following 72 hours after the contracted return date, has been discovered to have been stolen or

abandoned, or is the subject of an AMBER alert. In those circumstances, the rental company must maintain a record of information relevant to the activation of that technology.

Images and video recordings including individuals are typically considered to be more sensitive than diagnostic information concerning the general state of a vehicle (i.e. data collected by EDRs and SDMs), and personal vehicles are typically considered to garner a greater expectation of privacy than rental vehicles which do not belong to the renter. Accordingly, protections for image and video recording data collected in a personal vehicle should arguably be at least as strong as protections for EDR and SDM data, and at least as strong as protections for electronic surveillance data in rental vehicles. From a public policy standpoint, the bill in print seems to provide protections that would be coherent with such existing laws, whereas defaulting to the protections of the CCPA, which place few limitations on the collection of personal information and provide only the right to opt out of the sharing or sale of that personal information, seemingly would not (*see* Comment #4).

This bill seeks to provide privacy protections for data collected by in-vehicle cameras that are consistent with the level of sensitivity California law has thus far assigned to similar, albeit arguably less sensitive, data.

As Oakland Privacy argues in support of the bill:

Senate Bill 346 continues the Legislature’s consideration of enhanced privacy protections for particularly sensitive personal information. For many of us, our vehicles are places where we spend a great deal of time and the inside of it is a physical space considered fundamentally private, much like the inside of our own homes. We may engage in conversations about family business or our health, or participate in sensitive business-related meetings or conversations. We do not act in the space of our own private vehicles as if we are being overheard by third parties. Even more innocuous acts like the radio stations we choose to listen to, or the podcasts we select, are considered by the vehicle’s occupants as fundamentally private choices. Essentially, in-vehicle cameras are much like smart speaker devices, in that they are repositories of information from Californian’s private lives and activities. This is timely legislation.

- 4) CCPA and supplementary privacy policy:** In 2018, California enacted landmark privacy legislation, the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), giving consumers certain rights regarding their PI, including: (1) the right to know what PI is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age. The CCPA includes in its definition of PI “audio, electronic, visual, thermal, olfactory, or similar information,” which would likely capture images and recordings captured by in-vehicle cameras. (Civ. Code Sec. 1798.100, et seq.)

Accordingly, the protections provided by the CCPA are available with respect to recordings collected by in-vehicle cameras to the extent that the data are identifiable. The CCPA also provides a private right of action in the event a consumer’s nonencrypted and nonredacted PI is subject to unauthorized access, theft, or disclosure, which would apply if the unauthorized access, theft, or disclosure was the result of negligence by the business. (Civ. Code Sec. 1798.150.)

In opposition to this bill, the Alliance for Automotive Innovation (AAI), an organization representing manufacturers of motor vehicles, and TechNet, argue that the provisions of the bill in print would conflict with the CCPA and preclude access to its protections, thereby weakening consumer privacy. AAI and TechNet contend:

[B]y effectively creating a carve out to the CCPA, we believe that this bill diminishes existing privacy protections that apply to images and video recordings captured by in-vehicle cameras pursuant to that landmark, comprehensive privacy law – rights that apply in a technology- and industry- neutral manner to provide consumers with a bevy of privacy rights such as the right to delete, the right of access, and the right to be informed about the collection, sale, or sharing of personal information, among other things. In this regard, we believe that this bill poses a critical decision for the Legislature insofar as SB 346 essentially exempts this particular technology from the CCPA and sharply deviates from one of the major objectives of that law by returning to the case-by-case development of privacy protections specific to industries or technologies.

The CCPA provides minimum protections for PI generally, and as such, extends such protections to identifiable recordings collected by in-vehicle cameras, but it explicitly leaves room for further regulation in circumstances in which more extensive protection is necessary. Specifically, the CCPA includes provisions indicating that its protections for consumer privacy and data control should be interpreted broadly and should be in addition to, not in the place of, more specific consumer protections as circumstances demand. Section 1798.194 of the Civil Code, for instance, provides that the CCPA “shall be liberally construed to effectuate its purposes,” and Section 1798.175 of the Civil Code further provides:

[The CCPA] is intended to further the constitutional right to privacy and to supplement existing laws relating to consumers’ personal information [...] Wherever possible, law relating to consumers’ personal information should be construed to harmonize with provisions of [the CCPA], but in the event of a conflict between other laws and provisions of [the CCPA], the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

Furthermore, the California Privacy Rights Act (CPRA), passed by ballot initiative as Proposition 24 in 2020, which will supplement, and in some cases supplant, the CCPA in 2023, explicitly provides for amendment of its general privacy provisions so long as those changes further the protection of consumer privacy. Specifically, the text of Proposition 24 allows for amendment by the Legislature with a majority vote of both houses and the signature of the Governor, but only if “such amendments are consistent with and further the purpose and intent of this Act[...]” which is “to further protect consumers’ rights, including the constitutional right of privacy.” (Ballot Pamp., Primary Elect. (Nov. 3, 2020) Text of Proposed Laws, pp. 43-44, 74-75.)

Based on these provisions, it does not seem that privacy laws that supplement the protections provided in the CCPA in cases of particular sensitivity conflict with the purpose and intent of either the CCPA or the pending CPRA, nor would such a law necessarily be construed to deprive consumers of the protections under CCPA by expanding upon them.

Nonetheless, to ensure that the rights afforded by SB 346 would be in addition to, rather than in place of, the rights afforded by the CCPA/CPRA, the author has offered the following amendment:

Author's amendment #1:

On page 7, after line 35, insert: “**22948.57. (a) The provisions of this chapter shall not reduce the rights afforded to a consumer or the obligations imposed on a business under any applicable state or federal law for the protection of individual privacy.**

(b) In the event of a conflict between the provisions of this chapter and any other state law, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.”

On page 7, line 36, strike “22948.57” and insert: “**22948.58**”

- 5) **The bill in print would inform consumers of in-vehicle cameras upon purchase of a motor vehicle, and would limit the use, retention, and disclosure of resulting recordings:** SB 346 as it is currently in print seeks to protect the privacy of drivers by requiring a manufacturer of a new motor vehicle sold or leased in this state to disclose if the vehicle is equipped with one or more in-vehicle cameras either in the owner’s manual or in a document sent to the seller or leaser of the vehicle, as applicable, and requiring the seller or leaser to prominently inform, during the purchase of the vehicle, that it is equipped with one or more in-vehicle cameras in accordance with certain specifications. The bill also prohibits the use of recordings collected or retained by the manufacturer through operation of an in-vehicle camera for any advertising; selling recordings to third parties; sharing with third parties except with affirmative consent, upon proper notice, and exclusively for specified purposes; retaining recordings anywhere other than the vehicle itself without the user’s affirmative consent; and downloading, retrieving, or otherwise accessing recordings without the user’s affirmative prior consent. The bill requires that the person or entity providing the operation of an in-vehicle camera to provide effective mechanisms for a consumer to revoke their consent at any time after it is given, and to honor the consent revocation, and delete recordings associated with the user from all locations other than the vehicle itself, as soon as practicable, but not later than 30 days after the user revokes consent. The bill further prohibits a person or entity from compelling a manufacturer to build specific features into in-vehicle cameras for the purpose of allowing surveillance by law enforcement.

The sponsors of the bill, Consumer Federation of California, argue:

People often spend a significant portion of their days inside their car, whether it be a work commute, running errands, or simply a leisure drive. A car can often act as a second home, and, similar to when people are in their home, there is an expectation of privacy. [...] Consumers do not expect that buying a new car can also potentially mean opening up their private life to the car’s manufacturer. In fact, once the vehicle is sold, it would seem that the manufacturers’ right to any interior video should be extinguished. Privacy protections already exist for other kinds of technology that collect data in people’s private spaces. For example, certain voice recordings collected by smart TV’s inside of a person’s home are prohibited from being sold or used for advertising.

The amount of personal data collected through the use of new technologies is staggering and has come under scrutiny, leading to a push for further regulation. CFC believes that images collected by in-vehicle cameras are particularly sensitive and California should enact strong common sense rules to ensure that new technology or features do not come

at the expense of consumer privacy. Drivers and consumers deserve strong protections as vehicles and vehicle technology continue to evolve and change into the future.

The provisions of the bill in print seem to contemplate a number of potential harms consumers could experience if they are not adequately informed of the presence of an in-vehicle camera, and if there are not appropriate constraints on the use of that information. Accordingly, the bill would arguably better protect the revealing, sensitive personal information collected in the privacy of one's vehicle.

Opposing the bill unless amended, the California New Car Dealers Association (CNCDA) contend that the disclosure requirement of the bill would impose overly burdensome operational requirements on dealership employees that would differ from vehicle to vehicle, arguing:

The presence of an in-vehicle camera will differ not only from vehicle to vehicle, but from one vehicle trim level to the next. Requiring dealers to inform customers about the presence of any in-vehicle cameras during the vehicle purchase process will be extremely difficult to implement on a vehicle-by-vehicle basis, and this operational difficulty is especially acute with civil penalties attached. We have requested that the author amend the bill to direct dealers to provide notice to *all* customers and draw their attention to the fact that their vehicle may have an in-vehicle camera, and they should consult the owner's manual or manufacturer's website for more information.

Because the amendment suggested by CNCDA would result in provision of the same notice to all new vehicle buyers, whether or not the vehicle contains an in-vehicle camera, it would arguably provide minimal additional information, and would instead add additional paperwork of little value to an already complex vehicle-purchasing process. That said, the operational burden identified by CNCDA does seem to indicate that careful consideration of a disclosure process is necessary to ensure the consumer is adequately informed without excessively burdening new car dealers, many of which are small businesses.

To provide the opportunity for future legislation to contemplate and establish a practical and informative disclosure pertaining to in-vehicle cameras, the author has offered the following amendment, which would strike the disclosure requirement from the bill in its entirety:

Author's amendment #2:

On page 2, strike 7-10, inclusive.

Strike page 3 in its entirety.

- 6) **Opponents argue the bill in print is “lacking critical exemptions”:** Generally speaking, the CCPA includes various exemptions from the act, some of which exempt certain types of information more broadly, and others which apply to the extent that the CCPA would conflict with certain necessary actions of a business. For example, the CCPA specifically states that the obligations imposed by the act shall not restrict a business's ability to comply with federal, state, or local laws, or to exercise or defend legal claims. It also separately provides for certain broader exemptions, such as for medical information governed under the Confidentiality of Medical Information Act (CMIA) or federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), or for information covered under the Gramm-

Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (FIPA). These broader CCPA exemptions have largely been granted in recognition that there are already comprehensive state or federal laws providing privacy protections for that specific information, such as in the case of CMIA, HIPAA, or GLBA. The concern in those situations was that confusion could arise as businesses attempt to determine which law takes precedent under certain circumstances.

As it is currently in print, SB 346 does not make several of these same exemptions explicit. That said, several of the exemptions in the CCPA, which applies to data generally, are unlikely to be relevant in this narrower context of in-vehicle recordings. It does not seem appropriate to explicitly carve out potentially conflicting laws pertaining to medical information collected by health care providers or financial information collected by financial institutions, since neither fall under the scope of this bill. Rather, the bill permits images or video recordings retained through the operation of an in-vehicle camera to be retrieved or shared without the user's permission only if any of the following apply: 1) a court or other judicial or administrative authority authorizes the retrieval of the images or video recordings, and any images and video recordings retrieved are subject to the standards for admission into evidence required by the court or other administrative authority; 2) the images or video recordings are retrieved pursuant to an investigation or inspection pursuant to federal law authorizing the Secretary of Transportation and the National Transportation Safety Board, respectively, to investigate motor vehicle accident; or 3) the images or video recordings are retrieved for the purpose of immediately determining the need for, or facilitating, emergency medical response to a motor vehicle crash.

AAI and TechNet argue:

In contrast to the CCPA, SB 346 lacks critical exemptions that ensure workability and avoid undermining other important public policy goals. This includes situations where compliance with certain restrictions would create a conflict with a business's other legal obligations or prevent its compliance with legal orders, or otherwise hinder its ability to innovate, to name a few. This is most problematic with respect to the sharing restrictions. Such overly restrictive prohibitions against sharing, combined with other issues with the bill (such as its failure to clearly make a critical distinction between the handling of identifiable data that can be linked to a consumer and data that cannot), raise serious concerns about unreasonable interference with legitimate uses of this technology, both now and in the future.

Just consider the potential uses of images or video recordings that cannot reasonably be linked back to a particular individual:

- For non-commercial but publicly beneficial purposes, such as the National Highway Traffic Safety Administration's efforts around tracking and curbing drowsy driving.
- To improve technologies for the benefit of consumers, increasing reliability, helping prevent accidents or deaths, such as with autonomous vehicles.
- To conduct research and development that can lead to new, innovative technologies that we cannot even imagine today.
- To allow technology partners to fix security bugs or address defects.

- To enhance safety features.

Also consider situations where sharing identifiable video recordings or images may be warranted irrespective of a consumer's affirmative consent:

- To comply with a court order in connection with an investigation, lawsuit, or criminal proceeding.
- To share this data with law enforcement, such as in cases where a passenger has been assaulted by a driver or where it could assist victims of human trafficking or kidnapping.

All of the above uses would be prohibited under SB 346, without exception.

Staff notes that, contrary to the argument of the opponents, SB 346 does not appear to prohibit sharing of identifiable video recordings without the consumer's consent if a court order has been issued, including a warrant based on probable cause (e.g. in the case of suspected assault, human trafficking, or kidnapping), as it explicitly specifies "a court or other judicial or administrative authority authorizes the retrieval of the images or video recordings" as one of the conditions in which retrieval without consent is permissible.

Staff further notes that although opponents claim the bill would prohibit, without exception, use of in-vehicle camera recordings to improve technologies to prevent accidents or death, to allow technology partners to fix security bugs or address defects, and to enhance safety features, the exception to the prohibition on sharing appears to allow for use in these circumstances, so long as the user provides affirmative consent. Specifically, the bill allows for sharing of image or video recordings collected or retained through the operation of an in-vehicle camera with a third party if the user has provided affirmative consent; the images or recordings are only used to the extent necessary to improve portions of the vehicle's safety system that rely on or utilize the camera, or to diagnose, service, or repair the in-vehicle camera or vehicle equipment that relies on or utilizes the camera; and the recipient complies with certain notice, consent, and data minimization requirements.

Still, while the bill provides for retrieval or sharing of images or videos without user consent in the event of a court order or administrative order, it is not entirely clear whether this would include a valid public records request. In some circumstances, such as in cases of misconduct by law enforcement officials inside their vehicles, in-vehicle camera recordings may contain issues of public interest, and the rigid constraints imposed by this bill could consequently interfere with legitimate journalistic investigation.

Recognizing the importance of an unencumbered press, the author has agreed to the following amendments, to clarify the availability of in-vehicle camera footage in response to a public records request and to explicitly provide that the bill shall not be construed to interfere with legitimate journalistic activities:

Author's amendment #3:

On page 4, after line 30, insert: "***(C) The images or video recordings are shared with a third party pursuant to a public records request, including, but not limited to, a request***

pursuant to subdivision (b) of Section 832.7 of the Penal Code or paragraph (4) of subdivision (f) of Section 6254 of the Government Code.”

On page 7, after line 35 and after the provisions of author’s amendment #1, insert: “(c) *The rights afforded to consumers and the obligations imposed on any business under this chapter shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.*”

7) Anti-discrimination provision may preclude compliance by some manufacturers:

Similar to the CCPA, the bill in print would prohibit a person or entity from discriminating against a user because the user has exercised any of their rights under the bill, including, but not limited to: denying goods, services, or benefits to the user; charging different prices or rates for goods or services, including through the use of discounts or other incentives or imposing penalties; providing a different level or quality of goods, services, or benefits to the user; suggesting that the user will receive a different price, rate, or level or quality of goods, services, or benefits; or considering the user’s exercise of rights under the bill as a basis for suspicion of criminal wrongdoing or unlawful conduct.

Preventing discrimination on the basis of rights exercised is arguably a critical provision to ensure that consumers can avail themselves of those rights without fear of repercussions, and have the opportunity to provide or withhold real consent. In some cases, however, a particular function provided by the manufacture may rely on a practice that requires consent under the bill, and withholding consent would accordingly preclude or degrade the ability to provide that function. Inevitably, as a result of the consumer’s choice to withhold consent, the manufacturer would consequently be unable to provide the same level or quality of service, or in some cases, to provide the service at all, which would constitute discrimination under the bill in print.

An unintended consequence of this construction may therefore be that manufacturers would not be able to provide any service that can only be accomplished through a practice that requires the user’s consent under the bill, whether or not the user consents, as they would risk discrimination liability by degrading that service or denying that service should the user withhold consent. To resolve this issue, should the bill pass out of this Committee, as the bill moves through the Legislative process, the author may consider amending the bill to clarify that denying or providing a different quality of service does not constitute discrimination if a practice requiring the user’s consent is strictly necessary to provide that service, and the user withholds that consent.

8) Images and videos that “cannot reasonably be linked back to a particular individual”:

In opposition to the bill, AAI and TechNet contend that “the failure to clearly make a critical distinction between the handling of identifiable data that can be linked to a consumer and data that cannot [raises] serious concerns about unreasonable interference with legitimate uses of this technology.”

It is difficult to conceive of data that would constitute “images or video recordings” from inside a vehicle that would be of use to the manufacturer but do not constitute personal information, especially considering any such recording would be derived from a specific identifiable vehicle and personal information as it is defined in CCPA includes “audio, electronic, visual, thermal, olfactory, or similar information,” so long as it is reasonably

capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Given the vast troves of available personal information that can be collected or purchased by manufacturers, even data that has undergone some anonymization can often be readily re-identified in conjunction with other data or through the use of sophisticated algorithms, both of which can be withheld from public scrutiny as trade secrets under most circumstances. This is particularly true in light of the profound interest by data collection giants such as Google, Apple, and Amazon in entering the automobile market, either through software integration or hardware development.¹

Nonetheless, the ethics of surveillance in a place in which privacy is expected, even if that surveillance does not yield identifiable images or recordings, are not clear cut. Courts generally recognize two legally protected privacy interests: 1) “informational privacy,” or interests in precluding the dissemination or misuse of sensitive and confidential information, and; 2) “autonomy privacy,” or interests in making intimate personal decisions or conducting personal activities without *observation*, intrusion, or interference. (See, e.g., *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal. 4th 1, 35; emphasis added.) Case law provides that there is a legitimate expectation of privacy in the interior of a car (*People v. Bell* (1996) 43 Cal.App.4th 754, 770), but staff could not locate any case law that expounds on whether surveillance that cannot identify individuals in a location with a reasonable expectation of privacy violates a significant privacy interest.

By way of analogy, however, certain contexts can be envisioned in which the mere presence of a watcher can affect behavioral freedoms core to autonomy privacy, whether or not the data being collected is anonymized. For instance, rather than a camera being placed in the cabin of a car by a manufacturer, suppose a camera was placed by the government inside an individual’s home. Even if this placement was qualified by an alleged legal prohibition on the collection of personal information, an individual’s ability to behave freely within the confines of their home would depend on their trust in the camera provider’s compliance with the law, and would probably be affected even if their level of trust in that institution is high. Similarly, most individuals would likely be uncomfortable with a camera being placed in a public bathroom stall, even if the camera included a notice that any images of individuals would be blurred or otherwise obscured. These examples demonstrate that the presence of surveillance instruments in a context in which there is a reasonable expectation of privacy, whether or not they are collecting personal information, can affect behavior in a manner incompatible with the ethical foundation of the legal right to privacy.

Arguably, the reasonable expectation of privacy in a vehicle, particularly on public thoroughfares, is less pronounced than in a bathroom or one’s own home. Still, regulating only the collection of personal information, rather than all images and video recordings, within these private spaces risks a so-called panopticon effect –the fact that individuals cannot know when they are being watched means that they are motivated to act as though they are being watched at all times.

- 9) Author’s amendments:** In addition to the amendments offered in Comments #4, 5, and 6, the author has offered the following amendments to resolve technical issues within the bill.

¹ See, e.g., Leah Nysten, “Big Tech’s Next Monopoly Game: Building the Car of the Future,” *Politico Magazine*, Dec. 26, 2021, <https://www.politico.com/news/magazine/2021/12/27/self-driving-car-big-tech-monopoly-525867> [as of Jun. 19, 2022].

Author's amendment #4 serves to clarify that a court may enjoin a violation of the bill's provisions whether or not the violation is knowingly committed, and author's amendment #5 corrects an inconsistency within the bill's language to align the individual who can consent to allowing access to in-vehicle camera footage with the individual who can access the footage by default.

Author's amendment #4:

On page 7, line 20, strike the word "knowingly".

Author's amendment #5:

On page 4, line 34, strike "registered owner of the motor vehicle" and insert: "*user*".

10) Related legislation: AB 1262 (Cunningham) would establish limitations on the use, retention, sharing, and sale of recordings or transcriptions containing personal information collected by the voice recognition feature of a smart speaker device, and would prohibit a person or entity from providing the operation of a voice recognition feature without prominently informing the user during initial setup of a smart speaker device.

AB 2392 (Irwin) would specify that a manufacturer of a connected device satisfies existing law requiring the device to be equipped with reasonable security features if the connected device complies with a labeling scheme that conforms to criteria developed by the National Institute on Standards & Technology (NIST), as specified

SB 1172 (Pan) would require a business providing proctoring services in an educational setting to collect, use, retain, and disclose only the personal information strictly necessary to provide that service.

11) Prior legislation: AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment #4.

AB 213 (Leslie, Ch. 427, Stats. 2003) *See* Comment #3.

AB 2840 (Corbett, Ch. 317, Stats. 2004) *See* Comment #3.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Federation of California (sponsor)
Consumer Attorneys of California
Consumer Federation of America
Consumer Reports
Consumer Watchdog
Consumers for Auto Reliability and Safety (CARS)
Oakland Privacy
Privacy Rights Clearinghouse

Opposition

Alliance of Automobile Manufacturers

California New Car Dealers Association
TechNet

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200