Date of Hearing: March 26, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 814 (Chau) – As Introduced February 20, 2019

SUBJECT: Vehicles: unlawful access to computer systems

SUMMARY: This bill would provide that any person who knowingly and without permission accesses any computer system, data system, or software that is located within, connected to, or otherwise integrated with any motor vehicle, with the intent of obtaining or reviewing data, uploading data or code, damaging, or in any way manipulating or controlling any part of the vehicle or any display within the vehicle shall be punished by imprisonment or by a fine, or by both the fine and imprisonment, as specified.

EXISTING LAW:

1) Prohibits a person from willfully injuring or tampering with any vehicle or the contents thereof or breaking or removing any part of a vehicle without the consent of the owner. (Veh. Code Sec. 10852.)

2) Defines numerous computer or electronic data offenses and imposes a wide range of penalties based on the seriousness of the offense or based on the extent of harm caused by the defendant. These penalties apply where any person knowingly, among other things:

   - Accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort, or wrongfully control or obtain money, property, or data.

   - Accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

   - Accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

   - Without permission, disrupts or causes the disruption of computer services or denies or causes the denial of computer services, to an authorized user of a computer, computer system, or computer network.

   - Disrupts or improperly accesses a government or public safety computer system. (Pen. Code Sec. 502.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill would explicitly make the action of hacking into a vehicle's software without permission, a crime. This bill is author-sponsored.

2) **Author's statement**: According to the author, "[a]s automotive technology has progressed, the industry has made great strides in mobilizing and integrating advanced computer hardware into even the most basic automobiles. This has resulted in cleaner running, more efficient, more reliable, and perhaps most noticeably, more comfortable vehicles, to be manufactured and sold to consumers. These advancements, however, have opened up whole new avenues of risk and risk assessment. The hardware technologies required for these advancements are far more akin to the capabilities found in a high-powered home PC or smart phone than any vehicle most of people are familiar with, and bring with them all the same dangers for exploitation. A bad actor may access a vehicle's systems to download a record of the vehicle's location. They can also utilize the vehicle's onboard microphone to spy on unsuspecting occupants, or they may utilize the vehicle's wireless surface areas to simply steal the vehicle itself. AB 814 explicitly makes the unauthorized access of a vehicle's computer system, data system, or software, located within the vehicle, illegal under California [l]aw."

3) **Background**: In 2015, a pair of security experts remotely hacked into the wireless internet connection (Uconnect) of an unmodified 2014 Jeep Cherokee and took control of several of the vehicle's functions. The experts, fully authorized by the vehicle's owner, used laptop computers to enter the Jeep's electronic network and switched on the air conditioning, turned the radio up to full volume, and displayed an illustration of themselves on the vehicle's in-dash screen. The hack also gave them control of the door locks and throttle. In a parking lot, the hackers later showed how they could take control of the Cherokee's steering and brake systems. They were also able to turn the engine off and cause the vehicle to slowly drive into a ditch. (Andy Greenberg, *Hackers Remotely Kill A Jeep on the Highway - With Me In It*, Wired (Jul. 21, 2015), <https://www.wired.com/2015/07/hackers-remotely-kill-jeephighway/> [as of Mar. 15, 2019].)

   The Jeep Cherokee hack of 2015 proves that wireless attacks on connected vehicles are both achievable and real. Some suggest the risk of cyberattacks on autonomous vehicles are overblown, while others argue that the hijacking of autonomous vehicles could lead to terror on the scale of the September 11 attacks. (*See* Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 Wake Forest J.L. & POL'Y 339, 375 (2015); and William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 Santa Clara High Tech. L.J. 99, 133 (2015).)

   Within nine days after the Jeep incident, Fiat Chrysler issued a recall affecting 1.4 million vehicles with Uconnect technology including Dodges, Jeeps, Rams, and Chryslers. It was the first safety recall issued for a hacking threat, and brought immediate demands from legislators on Capitol Hill for action. (Kessler, *Fiat Chrysler Issues Recall Over Hacking*, New York Times (Jul. 24, 2015).) One of the debated pieces of legislation at the federal level would have capped a penalty for vehicle hacking at $100,000 and required the National

Highway Traffic Safety Administration (NHTSA) to establish an Automotive Cybersecurity Advisory Council. Another called for improved cybersecurity in connected vehicles. Ultimately those efforts went nowhere. In October of 2016, however, NHTSA did publish a guide to best practices in cybersecurity for vehicles. (NHTSA, *Cybersecurity best practices for modern vehicles* (Report No. DOT HS 812 333) (Oct. 2016).) In this document containing non-binding guidance, NHTSA describes the document's purpose as follows:

> Vehicles are cyber-physical systems and cybersecurity vulnerabilities could impact safety of life. Therefore, NHTSA's authority would be able to cover vehicle cybersecurity, even though it is not covered by an existing Federal Motor Vehicle Safety Standard at this time. Nevertheless, motor vehicle and motor vehicle equipment manufacturers are required by the National Traffic and Motor Vehicle Safety Act, as amended, to ensure that systems are designed free of unreasonable risks to motor vehicle safety, including those that may result due to existence of potential cybersecurity vulnerabilities.
>
> NHTSA believes that it important for the automotive industry to make vehicle cybersecurity an organizational priority. This includes proactively adopting and using available guidance such as this document and existing standards and best practices. Prioritizing vehicle cybersecurity also means establishing other internal processes and strategies to ensure that systems will be reasonably safe under expected real world conditions, including those that may arise due to potential vehicle cybersecurity vulnerabilities.
>
> The automotive cybersecurity environment is dynamic and is expected to change continually and, at times, rapidly. NHTSA believes that the voluntary best practices described in this document provide a solid foundation for developing a risk-based approach and important processes that can be maintained, refreshed and updated effectively over time to serve the needs of the automotive industry. (*Id.* at p.5.)

Rather than increasing the penalties after a vehicle has been unlawfully accessed, this guidance provided by NHTSA represents a front-end approach where vehicles should be equipped with adequate cybersecurity to prevent such unlawful access. In the absence of any other federal regulation, this non-binding guidance may be the most significant action that the federal government has taken regarding the cybersecurity of vehicles since 2015.

4) **Bill is consistent with existing law**: This bill would expressly prevent the unauthorized access of the computer system, data system, or software that is located within, connected to, or otherwise integrated with any motor vehicle. This is consistent with existing laws, which prohibit both tampering with a vehicle, and unauthorized access to a computer. (*See* Veh. Code Sec. 10852 and Pen. Code Sec. 502(d).)

California's vehicle tampering prohibition provides that "[n]o person shall either individually or in association with one or more other persons, wil[l]fully injure or tamper with any vehicle or the contents thereof or break or remove any part of a vehicle without the consent of the owner." (Veh. Code Sec. 10852.) This section has not been amended since its enactment in 1959, and it is likely that the Legislature did not anticipate the possibility of vehicle software and vehicle hacking at that time. However, it does not seem beyond the reach of the court to determine that injuring or tampering with a function of a vehicle through connected software would fall within the scope of the statute.

By comparison, California's Data Access Fraud law (CDAF), enacted in 1989, has been amended many times as the Legislature has grappled with the risks associated with the development of new technology. The act expresses the Legislature's intent to:

> [E]xpand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.
>
> The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data. (Pen Code Sec. 502(a).)

Consistent with the stated intent, the CDAF covers the unauthorized access of both hardware and software, and bases any penalties on the seriousness of the offense or on the harm caused by the defendant. These penalties apply where any person knowingly accesses a computer, computer system, or computer network, and without permission: (1) alters, damages, deletes, destroys, or otherwise uses any data in order to devise or execute any scheme or artifice to defraud, deceive, or extort, or wrongfully control or obtain money, property, or data; (2) takes, copies or makes use of any data, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network; (3) adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network; or (4) disrupts or causes the disruption of computer services or denies or causes the denial of computer services, or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

Thus, the CDAF clearly covers the knowing and unauthorized theft or destruction of any data held by a vehicle's computer system. It is not clear, however, that it would cover the knowing and unauthorized access of a vehicle's computer system (*e.g.*, the locking of a vehicle's doors) if that action was not part of a scheme to defraud or extort any money from the vehicle's owner. The remote and unauthorized locking of doors may very be in violation of the vehicle tampering statute, but at the time of this writing, it does not appear that any California courts have been faced with this particular question.

Accordingly, this bill would explicitly provide that any person who knowingly and without permission accesses any computer system, data system, or software that is located within, connected to, or otherwise integrated with any motor vehicle, with the intent of obtaining or reviewing data, uploading data or code, damaging, or in any way manipulating or controlling any part of the vehicle or any display within the vehicle is guilty of a crime. This should ensure that the unauthorized and knowing hacking of a vehicle, for *any* purpose, is prohibited under law. Under this bill, any person found to have violated this law would be subject to imprisonment in a county jail for not more than one year, or by a fine of not more than five $5,000, or by both the fine and imprisonment.

5) **Who has the authority to grant permission grant access to a vehicle's computer system**: After the Jeep Cherokee hack and the Fiat Chrysler automobile safety recall of nearly 1.4 million vehicles (*see* Comment 3, above), federal legislation was discussed that drew sharp criticism from the public. Specifically, the House Energy and Commerce Committee published draft legislation that would have made it illegal for anyone to hack a car, and some claimed that the prohibition would extend to owners or those conducting research on the vehicle. As noted in a Motherboard article:

> If we agree that cars are now computers, the future of car repair probably lies in its software. And if altering the software is "hacking," then […] this bill could more strictly narrow who is able to work on cars or point out their security flaws.
>
> The question this bill is asking, then, is who owns your car? Increasingly, manufacturers are arguing that while you may use their vehicles, the software that makes it run is theirs, and you are merely using it with their permission. (Koebler, *Congress's Car Hacking Bill Is a Complete Mess,* Motherboard (Oct. 22, 2015).)

This argument is largely a criticism of the Digital Millennium Copyright Act (DMCA), enacted by Congress in 1998 to prevent copyright infringement of digital copyrighted works. (DCMA, H.R. No. 2281, 105th Cong., 2nd Sess. (1998).) A large portion of the DMCA focuses on anti-circumvention laws intended to prevent copyright infringement by penalizing unauthorized users who circumvent or hack into copyrighted technology and software. Many security researchers believe that DMCA enforcement causes legal implications for security researchers who circumvent technology for good faith purposes. This good faith research includes attempting to find security glitches and solutions in vehicle software and medical implants to prevent hackers from accessing the information and using it dangerously.

In 2015, the DMCA was amended to allow circumvention of vehicle software for "diagnosis, repair, or lawful modification of a vehicle function[.]" (37 C.F.R. 210.40 (2015).) This amendment, however, did not address the question of whether it is the owner of a vehicle, or the manufacturer of the vehicle, who may authorize access to the vehicle's computer system. Further, the amendment was met with criticism from digital copyright owners and agencies, arguing that the exemption represents a dangerous slope that can facilitate copyright infringement and hacks.

For the purposes of AB 814, the DMCA as amended in 2015 would allow a vehicle owner to circumvent vehicle software (or authorize another to circumvent vehicle software) for the purposes of diagnosis or repair of the vehicle. The DMCA would not, however, permit a vehicle owner to authorize access to a vehicle's computer system for the purpose of research. Only the copyright owner (*i.e.*, the manufacturer) could grant that authorization.

6) **Prior legislation**: SB 30 (Gaines, 2015) would have expanded the methods by which carjacking can be accomplished to include remotely commandeering the vehicle through access of one or more of the vehicle's operating systems, as defined. This bill was never set for hearing in the Senate Public Safety Committee.

AB 1649 (Waldron, Ch. 379, Stats. 2014), specified the penalties for any person who disrupts or causes the disruption of, adds, alters, damages, destroys, provides or assists in providing a means of accessing, or introduces any computer contaminant into a "government computer system" or a "public safety infrastructure computer system," as specified.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Nichole Rapier / P. & C.P. / (916) 319-2200