SENATE COMMITTEE ON PUBLIC SAFETY

Senator Nancy Skinner, Chair
2019 - 2020 Regular

Bill No:	AB 814	**Hearing Date:**	June 4, 2019
Author:	Chau		
Version:	April 2, 2019		
Urgency:	No	**Fiscal:**	No
Consultant:	GC		

Subject: ***Vehicles: Unlawful Access to Computer Systems***

HISTORY

Source: Author

Prior Legislation: SB 30 (Gaines), 2015, failed passage in Senate Public Safety
AB 1649 (Waldron), Ch. 379, Stats. of 2014

Support: California District Attorneys Association

Opposition: None known

Assembly Floor Vote: 76 - 0

PURPOSE

This bill clarifies that existing law prohibits a person, business or government agency including a law enforcement agency, from hacking or otherwise accessing without authorization, computer data and computer systems in a motor vehicle.

Existing federal law makes it a crime to knowingly access a computer without authorization or exceeding authorized access. (18 U.S.C. § 1030.)

Existing law 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, § 10852.)

Existing law punishes the following offenses as a felony, by a fine not exceeding $10,000, by 16 months, two years or three years, or by both fine and imprisonment, or as a misdemeanor by a fine not exceeding $5,000, by imprisonment in a county jail not exceeding one year, or by both fine and imprisonment: (Pen. Code, § 502, subd. (d)(1).)

1) Any person who knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either devise or execute any scheme or artifice to defraud, deceive, or extort, or wrongfully control or obtain money, property, or data; (Pen. Code, § 502, subd. (c)(1).)

2) Any person who knowingly 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; (Pen. Code, § 502, subd. (c)(2).)

3) Any person who knowingly 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; (Pen. Code, § 502, subd. (c)(4).)

4) Any person who knowingly and 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; (Pen. Code, § 502, subd. (c)(5).)

5) Any person who knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network; (Pen. Code, § 502, subd. (c)(10).)

6) Any person who knowingly 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 public safety infrastructure computer system computer, computer system, or computer network; and, (Pen. Code, § 502, subd. (c)(11).)

7) Any person who knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network; (Pen. Code, § 502, subd. (c)(12).)

Existing law punishes any person who knowingly and without permission uses or causes to be used computer services as follows: (Pen Code, § 502(c)(3).)

1) For the first violation that does not result in injury, and where the value of the computer services used does not exceed nine hundred fifty dollars ($950), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and, (Pen. Code, § 502, subd. (d)(2).)

2) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds nine hundred fifty dollars ($950), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code, § 502, subd. (d)(2).)

Existing law punishes any person who knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network as follows: (Pen. Code, § 502, subd. (c)(6).)

1) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000);

2) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding

five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and,

3) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code, § 502, subd. (d)(3).)

Existing law punishes any person who knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network as follows: (Pen. Code, § 502, subd. (c)(7).)

1) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000);

2) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and,

3) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code, § 502, subd. (d)(3).)

Existing law punishes any person who knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network as follows: (Pen. Code, § 502, subd. (c)(13).)

1) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000);

2) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and,

3) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code, § 502, subd. (d)(3).)

Existing law punishes any person who knowingly introduces any computer contaminant into any computer, computer system, or computer network as follows: (Pen. Code, § 502, subd. (c)(8).)

1) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and,

2) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or by imprisonment, or by both that fine and imprisonment. (Pen. Code, § 502, subd. (d)(4).)

Existing law punishes any person who knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network as follows: (Pen. Code, § 502, subd. (c)(14).)

1) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and,

2) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or by imprisonment, or by both that fine and imprisonment. (Pen. Code, § 502, subd. (d)(4).)

Existing law punishes any person who knowingly and without permission uses the internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network. (Pen. Code, § 502(c)(9).)

1) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000); and,

2) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code, § 502, subd. (d)(5).)

Existing law defines the following terms as follows:

1) "Access" means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network. (Pen. Code, § 502, subd. (b)(1).)

2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities. (Pen. Code, § 502, subd. (b)(2).)

3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions. (Pen. Code, § 502, subd. (b)(3).)

4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network. (Pen. Code, § 502, subd. (b)(4).)

5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control. (Pen. Code, § 502, subd. (b)(5).)

6) "Government computer system" means any computer system, or part thereof, that is owned, operated, or used by any federal, state, or local governmental entity. (Pen. Code, § 502, subd. (b)(6).)

7) "Public safety infrastructure computer system" means any computer system, or part thereof, that is necessary for the health and safety of the public including computer systems owned, operated, or used by drinking water and wastewater treatment facilities, hospitals, emergency service providers, telecommunication companies, and gas and electric utility companies. (Pen. Code, § 502, subd. (b)(7).)

8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device. (Pen. Code, § 502, subd. (b)(8).)

9) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software. (Pen. Code, § 502, subd. (b)(9).)

10) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program. (Pen. Code, § 502, subd. (b)(10).)

11) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access. (Pen. Code, § 502, subd. (b)(11).)

12) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record,

or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network. (Pen. Code, § 502, subd. (b)(12).)

13) "Internet domain name" means a globally unique, hierarchical reference to an internet host or service, assigned through centralized internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy. (Pen. Code, § 502, subd. (b)(13).)

14) "Electronic mail" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable or receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval. (Pen. Code, § 502, subd. (b)(14).)

15) "Profile" means either of the following:

    a) A configuration of user data required by a computer so that the user may access programs or services and have the desired functionality on that computer; or,

    b) An internet website user's personal page or section of a page that is made up of data, in text of graphical form, that displays significant, unique, or identifying information, including, but not limited to, listing acquaintances, interests, associations, activities, or personal statements. (Pen. Code, § 502, subd. (b)(15).)

This bill specifies 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 as "hacking" or unauthorized access to computers, computer systems and computer data under California law.

COMMENTS

1. Need for This Bill

According to the author:

> As 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.
>
> Technologies that were once only found in DARPA laboratories or in science fiction are now standard features on a host of cars. Advanced collision avoidance systems that use complex algorithms to interpret sonar, Lidar, and optical inputs to avoid accidents, maintain speed, and perhaps one day take over for human drivers, are "standard equipment" on large numbers of cars and required on new vehicles in more than 40 countries by 2022. Higher-end models allow a user to

turn their car into a Wi-Fi hotspot, utilize sensors to track tire pressure, and relay that information wirelessly to a vehicle's engine control unit. Manufactures have even made the FM radio "smart" by allowing for limited data transmission using FM band radios.

Like all things however, these advancements 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 amends Penal Code section 502 to explicitly include in the definition of "computer system," any "device or system that is located within, connected to, or otherwise integrated with, any motor vehicle," for purposes of the prohibitions on unauthorized access to a computer system.

2. Advances in Vehicle Technology

According to the background provided by the author, technologies that were once only found in DARPA[1] laboratories or in science fiction are now standard features on a host of cars. Advanced collision avoidance systems that use complex algorithms to interpret sonar, Lidar, and optical inputs to avoid accidents, maintain speed, and perhaps one day take over for human drivers, are 'standard equipment' on large numbers of cars and required on new vehicles in more than 40 countries by 2022.[2] Higher-end models allow a user to turn their car into a Wi-Fi hotspot, utilize sensors to track tire pressure, and relay that information wirelessly to a vehicle's engine control unit. Manufactures have even made the FM radio 'smart' by allowing for limited data transmission using FM band radios.

Like all things however, these advancements 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.[3]

The public has been on notice of this problem for many years now. In 2015, the *Los Angeles Times* reported, "Just about any new car can be hacked — some even driven by remote control — as automakers depend more on software and wireless connections. Vehicle vulnerability may

[1] Defense Advanced Research Projects Agency - DARPA
[2] https://abcnews.go.com/Business/wireStory/40-countries-agree-cars-automatic-braking-61030078
[3] https://www.securitynewspaper.com/2018/10/25/hackers-steal-a-tesla-model-s-using-just-a-tablet/, https://www.businessinsider.com/smart-cars-are-vulnerable-to-hackers-2015-7, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, Car Hacking: The Content By Chris Valasek & Charlie Miller

only grow as cars become their own wireless hot spots with the advent of automated braking and steering systems, experts warn."[4] In 2016, the *Associated Press* reported on the vulnerability of vehicles key systems being computerized reporting that "[a] group of computer security experts say they figured out how to hack the keyless entry systems used on millions of cars, meaning that thieves could, in theory, break in and steal items without leaving a broken window."[5]

A recent article by the New York Times reports an instance of car hacking from 2010, where a former employee of the Texas Auto Center used a co-worker's account to log into company software used to repossess cars and hacked the software of over 100 cars, causing the vehicles to honk continuously and preventing them from starting.[6] The *Times* also reports on more pressing concerns: "Digital threats to self-driving cars, according to a 2018 University of Michigan report, 'include hackers who would try to take control over or shut down a vehicle, criminals who could try to ransom a vehicle or its passengers and thieves who would direct a self-driving car to relocate itself to the local chop-shop.' The average car has over 150 million lines of computer code…."

The most effective solution to the risk of cars being hacked is for automakers to ensure that software and computer systems in vehicles are safe from hacking. Notwithstanding that fact, it is and should be unlawful to hack a person's vehicle.

3. Hacking of Vehicles

California and the federal government have both criminalized the act of "hacking" or to (1) knowingly access a computer, system, or network (2) without the permission of the owner. (Penal Code § 502, subd. (c); and 18 U.S.C. 1030.)

The California Penal Code criminalizes the unauthorized taking or copying of data and information from a computer, computer system, or computer network. Depending on the criminal history of the defendant and the specific facts of the crime, this computer crime can be charged as either a felony or a misdemeanor. A misdemeanor conviction for this crime could result in a jail term of up to a year. A felony conviction could result in up to three years in prison.

Federal hacking provisions involve wrongfully accessing a computer or personal data on a computer without the owner's permission. A conviction for this crime carries a potential sentence of 10 years in federal prison.

This bill clarifies existing law, that the computer systems in a vehicle are computer systems for purposes of hacking provisions.

-- END –

[4] Jerry Hirsch, *Hackers Can Now Hitch a Ride on Car Computers*, Los Angeles Times, September 13, 2015, Available at: https://www.latimes.com/business/autos/la-fi-hy-car-hacking-20150914-story.html.
[5]Associated Press, *Millions of Cars' Keyless Entry Systems can be Hacked, Security Experts Find*, Los Angeles Times, August 12, 2016, Available at: https://www.latimes.com/business/autos/la-fi-hy-cars-hackers-20160812-snap-story.html.
[6]Jim Motavalli, *Locking More Than the Doors as Cars Become Computers on Wheels*, New York Times, March 7, 2019, Available at: https://www.nytimes.com/2019/03/07/business/car-hacks-cybersecurity-safety.html.