SENATE COMMITTEE ON PUBLIC SAFETY

Senator Nancy Skinner, Chair
2019 - 2020 Regular

Bill No:	SB 922	**Hearing Date:**	May 20, 2020
Author:	Chang		
Version:	February 4, 2020		
Urgency:	No	**Fiscal:**	No
Consultant:	SC		

Subject: ***Criminal Procedure: Limitations of Actions***

HISTORY

Source: Conference of California Bar Associations

Prior Legislation: SB 239 (Chang), held in Asm. Approps. Comm., 2019

Support: Alameda County District Attorney; California District Attorneys Association; California Police Chiefs Association; California State Sheriffs' Association; Los Angeles County District Attorney's Office; Peace Officers Research Association; Riverside Sheriffs' Association

Opposition: California Attorneys for Criminal Justice

As Proposed to be Amended in Committee

PURPOSE

The purpose of this bill is to amend the statute of limitations for felony offenses related to unlawful access of computer services and systems and extortion by ransomware.

Existing law provides that prosecution for crimes punishable by imprisonment for eight years or more and not otherwise covered must be commenced within six years after commission of the offense. (Pen. Code, § 800.)

Existing law provides that prosecution for other felonies punishable by less than eight years must be commenced within three years after commission of the offense. (Pen. Code, § 801.)

Existing law provides that prosecution for crimes involving fraud, breach of a fiduciary duty, embezzlement of funds from an elder or dependent adult, or misconduct by a public official does not start to run until the discovery of the offense and prosecution must be commenced within four years after discovery of the crime or within four years after completion, whichever is later. (Penal Code § 801.5 & 803, subd. (c).)

Existing law states that prosecution for a misdemeanor shall be commenced within one year after the commission of the offense, unless otherwise specified. (Pen. Code, § 802, subd. (a).)

Existing law specifies that the statute of limitations for misdemeanors related to unlawful business practices and license violations is within three years after discovery of the commission of the offense, or within three years after completion of the offense, whichever is later. (Pen. Code, § 802, subd. (e).)

Existing law provides that unless provided, as specified, a limitation of time is not tolled or extended for any reason. (Penal Code § 803, subd. (a).)

Existing law provides that if more than one statute of limitations period applies to a crime, the time for commencing an action shall be governed by the period that expires later in time. (Penal Code § 803.6, subd. (a).)

Existing law states that, except as otherwise provided, prosecution for an offense is commenced when any of the following occurs:

- An indictment or information is filed;
- A complaint is filed charging a misdemeanor or infraction;
- The defendant is arraigned on a complaint that charges the defendant with a felony; or,
- An arrest warrant or bench warrant is issued, provided the warrant names or describes the defendant with the same degree of particularity required for an indictment, information, or complaint. (Pen. Code, § 804.)

Existing law states that for purposes of determining the applicable limitation of time the following apply:

- An offense is deemed punishable by the maximum punishment prescribed by statute for the offense, regardless of the punishment actually sought or imposed. Any enhancement of punishment prescribed by statute shall be disregarded in determining the maximum punishment prescribed by statute for an offense;
- The limitation of time applicable to an offense that is necessarily included within a greater offense is the limitation of time applicable to the lesser included offense, regardless of the limitation of time applicable to the greater offense. (Pen. Code, § 805.)

Existing law provides that the following conduct is an alternate felony-misdemeanor punishable by 16 months, two or three years in county jail and a fine of up to $10,000 or up to one year in county jail and by a fine of up to $1,000:

- Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;
- 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;

- 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;

- 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;

- 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;

- 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,

- 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.)

Existing law provides that a person who knowingly and without permission uses or causes to be used computer services shall be punished as follows:

- For the first violation that does not result in injury, and where the value of the computer services used does not exceed $950, as a misdemeanor punishable by a fine not exceeding $5,000 and by imprisonment in a county jail not exceeding one year; or

- For any violation that results in a victim expenditure in an amount greater than $5,000 or in an injury, or if the value of the computer services used exceeds $950, or for any second or subsequent violation, as an alternate felony-misdemeanor punishable by a fine not exceeding $10,000 and by imprisonment in county jail for 16 months, or two or three years, or by a fine not exceeding $5,000 and by imprisonment in a county jail not exceeding one year. (*Id.*)

Existing law provides that a person who (A) knowingly and without permission provides or assists in providing a means of accessing a computer, computer system or computer network, (B) knowingly and without permission accesses or causes to be accessed a computer, computer system or computer network, or (C) knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer, computer system or computer network shall be punished as follows:

- For a first violation that does not result in injury, an infraction punishable by a fine not exceeding $1,000;

- For any violation that results in a victim expenditure in an amount not greater than $5,000, or for a second or subsequent violation, as a misdemeanor by a fine not exceeding $5,000 and imprisonment in county jail for up to one year; or,

- For any violation that results in a victim expenditure in an amount greater than $5,000, as an alternate felony-misdemeanor punishable by a fine not exceeding $10,000 and by imprisonment in county jail for 16 months, or two or three years, or by a fine not exceeding $5,000 and by imprisonment in a county jail not exceeding one year. (*Id*.)

Existing law provides that a person who either (A) knowingly introduces any computer contaminant into any computer, computer system, or computer network, or (B) knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network shall be punished as follows:

- For a first violation that does not result in injury, as a misdemeanor punishable by a fine not exceeding $5,000 and by imprisonment in a county jail not exceeding one year; or,

- For any violation that results in injury, or for a second or subsequent violation, as an alternate felony-misdemeanor punishable by a fine not exceeding $10,000, and by imprisonment in a county jail not exceeding one year, or by imprisonment in county jail for 16 months, or two or three years. (*Id*.)

Existing law provides that 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 shall be punished as follows:

- For a first violation that does not result in injury, an infraction punishable by a fine not exceeding $1,000; or,

- For any violation that results in injury, or for a second or subsequent violation, as misdemeanor by a fine not exceeding $5,000 and by imprisonment in a county jail not exceeding one year. (*Id*.)

Existing law authorizes the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss due to a violation of Penal Code section 502 to bring a civil action against the violator for compensatory damages and injunctive or other equitable relief. (Pen. Code, § 502, subd. (e)(1).)

Existing law provides that any civil action seeking for a violation of Penal Code section 502 must be initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later. (Pen. Code, § 502, subd. (e)(5).)

Existing law provides that every person who with intent to extort property or other consideration form another, introduces ransomware into any computer, computer system or network, is guilty of a felony punishable by imprisonment in county jail. (Pen. Code, § 523, subd. (b)(1).)

Existing law defines "ransomware" to mean "a computer contaminant, as defined in Section 502, or lock placed or introduced without authorization into a computer, computer system, or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the placement or introduction of the ransomware demands payment of money or other consideration to remove the computer contaminant, restore access to the computer,

computer system, computer network or data, or otherwise remediate the impact of the computer contaminant or lock." (Pen. Code, § 523, subd. (c)(1).)

This bill amends the statute of limitations for felony violations of unlawful access of computer services and systems and extortion by introduction of ransomware which currently is three years after the commission of the offense to three years after discovery of the commission of the offense.

This bill specifies that the amended statute of limitations applies to crimes committed on or after January 1, 2021, and to crimes for which the statute of limitations that was in effect prior to January 1, 2021, has not elapsed as of January 1, 2021.

COMMENTS

1. Need for This Bill

According to the author:

> Crimes committed in cyberspace have real world consequences. From frozen bank accounts to destroyed or damaged files, cybercrimes have grown in scope and frequency. Apart from conventional hacking attacks, cybercriminals have resorted to using ransomware to extort large sums of money from victims in order to regain access to stolen assets.
>
> Hackers and cybercriminals are targeting individuals and families, small businesses and large corporations, and even entire municipalities. Hackers and their crimes become more brazen when they are failed to be apprehended and prosecuted. SB 922 is a step in the right direction towards holding hackers and cybercriminals accountable.
>
> Under existing law, the statute of limitations for digital crimes that involve a breach of trust (e.g., grand theft, identity theft, fraud, forgery, perjury, etc.) is four years after discovery of the offense, or four years after its completion, whichever is later.
>
> Similarly, the statute of limitations for computer hacking is three years after discovery, if prosecuted civilly. But, the statute of limitations for computer hacking prosecuted as a felony commences from the date of the offense -- not the date of discovery -- which is inconsistent and counterintuitive.
>
> This bill would allow the same statute of limitations for a felony violation of specified cybercrimes as a civil prosecution for the same act, i.e. three years after the date of discovery rather than the date of the offense.

2. Statutes of Limitations

Statutes of limitations require commencement of a prosecution within a certain period of time after the commission of a crime. A prosecution is initiated by filing an indictment or information, filing a complaint, certifying a case to superior court, or issuing an arrest or bench warrant.

(Penal Code § 804.) The failure of a prosecution to be commenced within the applicable period of limitation is a complete defense to the charge. The statute of limitations is jurisdictional and may be raised as a defense at any time, before or after judgment. (*People v. Morris* (1988) 46 Cal.3d 1, 13.) The defense may only be waived under limited circumstances. (See *Cowan v. Superior Court* (1996) 14 Cal.4th 367.)

The Legislature enacted the current statutory scheme regarding statutes of limitations for crimes in 1984 in response to a report of the California Law Revision Commission:

> The Commission identified various factors to be considered in drafting a limitations statute. These factors include: (a) *The staleness factor*. A person accused of crime should be protected from having to face charges based on possibly unreliable evidence and from losing access to the evidentiary means to defend. (b) *The repose factor*. This reflects society's lack of a desire to prosecute for crimes committed in the distant past. (c) *The motivation factor*. This aspect of the statute imposes a priority among crimes for investigation and prosecution. (d) *The seriousness factor*. The statute of limitations is a grant of amnesty to a defendant; the more serious the crime, the less willing society is to grant that amnesty. (e) *The concealment factor*. Detection of certain concealed crimes may be quite difficult and may require long investigations to identify and prosecute the perpetrators.
>
> The Commission concluded that a felony limitations statute generally should be based on the seriousness of the crime. Seriousness is easily determined based on classification of a crime as felony or misdemeanor and the punishment specified, and a scheme based on seriousness generally will accommodate the other factors as well. Also, the simplicity of a limitations period based on seriousness provides predictability and promotes uniformity of treatment.
>
> The Commission's recommendation that the statute of limitation period should correspond to the seriousness of the crime would best be effectuated by a one-year period for misdemeanors, a three-year period for most felonies, a six-year period for felonies punishable by eight or more years imprisonment), and no limitation for capital crimes or crimes punishable by life imprisonment.
>
> As to tolling of the statute of limitations until discovery of the offense, the Commission noted that tolling is appropriate for crimes where a material element is fraud or breach of a fiduciary obligation, *however tolling should not be permitted to run indefinitely*. The Commission recommended that a crime to which tolling applies should not be subject to prosecution more than nine years after it is committed and that such a limit would be a reasonable balance of interests. [1]

The United States Supreme Court has stated that statutes of limitations are the primary guarantee against bringing overly stale criminal charges. (*United States v. Ewell* (1966) 383 U.S. 116, 122.) There is a measure of predictability provided by specifying a limit beyond which there is an irrebutable presumption that a defendant's right to a fair trial would be prejudiced. Such laws reflect legislative assessments of relative interests of the state and the defendant in administering and receiving justice: "Significantly, a statute of limitations reflects a legislative judgment that,

[1] 1 Witkin Cal. Crim. Law Defenses, Section 214 (3rd Ed. 2004), citing 17 Cal. Law Rev. Com. Reports, pp.308-315.

after a certain time, no quantum of evidence is sufficient to convict. And that judgment typically rests, in large part, upon evidentiary concerns – for example, concern that the passage of time has eroded memories or made witnesses or other evidence unavailable. (*Stogner v. California* (2003) 539 U.S. 607, 615.)

Generally, the statute of limitations for misdemeanor offenses requires commencement of prosecution within one year of the commission of the offense (Pen. Code § 802) and for felony offenses, within three years of the commission of the offense (Pen. Code § 801). There are specified exceptions that either provides for a longer statute of limitations (Pen. Code, §§ 801.5, 802), tolls the time that the statute starts to run such as when the crime is discovered (Pen. Code § 803), or provides no statute of limitations at all (Pen. Code § 799).

This bill specifies for felony computer crimes listed in Penal Code section 502 and for extortion by ransomware the statute of limitations is three years after discovery of the commission of the offense. As stated by the author of this bill, the purpose of this change is to allow the same statute of limitations for felony violations of specified computer crimes as a civil prosecution for the same act or similar act. This timeframe is also similar to statutes of limitations for fraud-related offenses and specified misdemeanors related to unlawful business practices and license violations (4 years, and 3 years respectively, after the date of discovery of the offense or after the completion of the offense, whichever is later). (Pen. Code, §§ 801.5, 803, 802, subd. (e).)

However, as discussed in the Law Review Commission's report, tolling the statute of limitations indefinitely may not be reasonable when balancing all of the interests that must be considered when determining an appropriate limitation. The Commission recommended that statutes of limitations should not be allowed to toll for more than 9 years for a felony.

3. Effect of this Legislation

The effect of this change is that the statute of limitations would be longer than the current limit and potentially allow prosecution of cases many years after the crime was committed depending on when the crime is discovered. However, courts have interpreted the date of discovery provision of statutes of limitations to require due diligence in the investigative efforts of the crime. (*People v. Zamora* (1976) 18 Cal.3d 538, 561; *People v. Lopez* (1997) 52 Cal.App.4th 233, 246.) Thus, "discovery of the offense" is not synonymous with the date that the victim gained actual knowledge of the crime. (*People v. Zamora, supra*, 18 Cal.3d at 571.) "The crucial determination is whether law enforcement authorities or the victim had actual notice *of circumstances sufficient to make them suspicious of fraud thereby leading them to make inquiries which might have revealed the fraud*. (*Id*. at 572, original italics.) The identity of the perpetrator of the crime is not an element of the discovery issue. (*People v. Crossman* (1986) 210 Cal. App. 3d 476, 481.)

So while it is possible that the crimes affected by this bill could be prosecuted many years after their commission, the prosecutor would have the burden to prove by a preponderance of the evidence that the prosecution of the crime began within the required time which includes consideration of when the victim or law enforcement was aware of facts that would have alerted a reasonably diligent person in the same circumstances that a crime may have been committed. (CALCRIM No. 3410.)

4. Ex Post Facto

In *Stogner v. California, supra*, 539 U.S. 607 the Supreme Court ruled that a law enacted after expiration of a previously applicable limitations period violates the Ex Post Facto Clause when it is applied to revive a previously time-barred prosecution. (*Id*. at pp. 610-611, 616.) However, extension of an existing statute of limitations is not ex post facto as long as the prior limitations period has not expired. (*Id*. at pp. 618-619.) Existing statutory law also provides that any change in the time period for the commencement of prosecution applies to any crime if prosecution for the crime was not barred on the effective date of the change by the statute of limitations in effect immediately prior to the effective date of the change. (Pen. Code § 803.6, subd. (b).)

Under these principles, the amended statute of limitations provided for in this bill cannot be applied to cases in which the statute of limitations period has expired. This bill specifies that the amended statute of limitations applies to crimes committed on or after January 1, 2021 and to crimes for which the statute of limitations that was in effect prior to January 1, 2021, has not elapsed as of January 1, 2021.

5. Proposed Amendment

The committee amendment would limit the total time the statute of limitations may be tolled to no more than 9 years after the commission of the offense:

> 801.7. (a) Notwithstanding Section 801 or any other law, prosecution for a felony offense described in Section 502 or subdivision (b) of Section 523 shall be commenced within three years after discovery of the commission of the offense**, provided, however, that in any case a complaint may not be filed more than nine years after the commission of the offense.**
>
> (b) This section applies to crimes that are committed on or after January 1, 2021, and to crimes for which the statute of limitations that was in effect prior to January 1, 2021, has not elapsed as of January 1, 2021.

6. Argument in Support

According to the Conference of California Bar Associations, the sponsor of this bill:

> SB 922 will align the statute of limitations for felony computer hacking and felony extortion by ransomware with those of similar crimes by permitting prosecution three years after the date of discovery of the offense. Currently, the statute of limitations runs from the date when the offense occurred, which is often not ascertainable.
>
> Perpetrators of data breaches go to great lengths to conceal their crimes and thus victims are often unaware that a crime has been committed. For example, the 2013 Yahoo email hack that compromised over a billion accounts was not discovered until 2016, too late to prosecute criminally under the statute.
>
> Similarly, perpetrators of ransomware have extorted individuals and organization of every stripe, including hospitals, law offices, and local governments, by infecting their computer systems with specialized malware that will encrypt the

> victim's data and render it inaccessible without a cryptographic key. Under Penal Code section 523(b), the extortion by ransomware occurs when it is "introduced" into a computer system, rather than when the computer program holds the data hostage and demands payment. Unfortunately, data that is encrypted is impervious to forensic analysis that might reveal when ransomware was first "introduced." Thus, in order to prosecute extortion by ransomware, the statute of limitations needs to be tolled until the date of discovery of the offense, as the burden is on the prosecution to show that the charge was filed within the statute of limitations.
>
> . . . .
>
> SB 922 will address the problems posed by surreptitious computer hacking and the introduction of ransomware into computer systems by establishing the same statute of limitations for a civil prosecution under Penal Code section 502, i.e. three years after the date of discovery.

7. Argument in Opposition

California Attorneys for Criminal Justice writes:

> As drafted, SB 922 would permit the three-year statute of limitations for violations of Penal Code §§ 502 and 523(b) to toll from the date the alleged criminal behavior is discovered as opposed to when the conduct occurred. Penal Code §502 (unauthorized computer access and fraud) lists 14 separate computer-related offenses. Except where fraud is involved (see below), each of these 14 crimes are capable of discovery in the existing three-year statute of limitations with the most basic diligence and investigation. These crimes – unlawful disruption of public safety infrastructure computer services, unpermitted access to computer services, unpermitted data alteration, etc. – are all acts that can and should be discovered, investigated, and prosecuted within a three-year window.
>
> . . . .
>
> The statute of limitations serves an important role in the criminal justice system by requiring that the government pursue criminal prosecutions in a timely fashion. It is a rule of fundamental fairness. Delayed prosecutions harm both victims and defendants through the loss and/or deterioration of relevant evidence. The defense is particularly impacted by late prosecutions. The defendant is typically only made aware of the accusations against him/her at the conclusion of a government investigation and at the point at which he/she has been arrested or charged with a crime. As such, the defense is often at a disadvantage when it come to their ability to locate and preserve evidence in support of the defense. And the longer a prosecution is delayed, the greater the prejudice to the defense. Here, the expansion of the statute of limitations proposed by SB 922 is neither necessary nor wise.

-- END –