SENATE COMMITTEE ON PUBLIC SAFETY

Senator Steven Bradford, Chair
2021 - 2022 Regular

Bill No:	AB 1247	**Hearing Date:**	July 6, 2021
Author:	Chau		
Version:	May 24, 2021		
Urgency:	No	**Fiscal:**	No
Consultant:	SC		

Subject: ***Criminal procedure: limitations of actions***

HISTORY

Source: Conference of California Bar Associations

Prior Legislation: SB 922 (Chang), held in Assem. Approps., 2020
SB 239 (Chang), held in Assem. Approps., 2019
AB 32 (Waldron), Ch. 614, Stats. 2015
AB 1649 (Waldron), Ch. 379, Stats. 2014

Support: California District Attorneys Association; California State Sheriffs' Association; National Insurance Crime Bureau

Opposition: None known

Assembly Floor Vote: 78 - 0

PURPOSE

The purpose of this bill is to allow for the tolling of the statute of limitations for the prosecution of a felony offense for unlawful access of computer services until the discovery of the commission of the offense, or within three years that the offense could have reasonably been discovered, but no more than six years from the commission of the offense.

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).)

This bill amends the existing statute of limitations that applies to the prosecution for a felony violation for unlawful access of computer services to authorize the prosecution to be commenced within 3 years after discovery of the commission of the offense, or within 3 years after the offense could have reasonably been discovered, provided however, that the filing of a criminal complaint shall not be filed more than six years after the commission of the offense.

This bill specifies that the amended statute of limitations applies to crimes committed on or after January 1, 2021.

COMMENTS

1. Need for This Bill

According to the author of this bill:

> Under existing law, the statute of limitations for 'white-collar' 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. For example, the hacking attacks on Yahoo, which compromised more than 1.5 billion user accounts, occurred in 2013 and 2014 but were not revealed until later in 2016.
>
> Because computer criminals often take great steps in attempting to conceal their crimes, it may be too late to prosecute and hold cybercriminals accountable once they are discovered. The pandemic has had a visible toll on a business's ability to keep their doors open, suffering a cyber-attack and not having the financial means to fight it will permanently close their doors. With so many having to work remotely, it is not yet understood how many people are going to be affected in the coming months, and years, or the extent of data breaches occurring during this time.
>
> AB 1247 would ensure that victims do not feel powerless and that they have enough time to seek out remedies for having their personal information stolen by aligning the statute of limitations for felony computer hacking with a civil prosecution for the same, by allowing for criminal prosecution within three years of the date of discovery, rather than the date of the offense; or within three years after the offense could have reasonably been discovered.

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.

(Witkin Cal. Crim. Law Defenses, Section 214 (3rd Ed. 2004), citing 17 Cal. Law Rev. Com. Reports, pp.308-315.) 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, 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, that the statute of limitations is three years after discovery of the commission of the offense or three years after the offense could have been reasonably discovered. However, regardless of the tolling provision, a criminal complaint shall not be filed later than six years after the commission of the offense. As stated by the author of this bill, this change would align the statute of limitations for felony violations of specified computer crimes as is currently allowed for 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).)

3. Effect of this Legislation

The effect of the change made by this bill 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.)

Thus, the prosecutor has 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.)

This bill clarifies that the tolled statute of limitations applies to when the offense could have reasonably been discovered, which may be an earlier timeframe that when the offense was actually discovered.

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, any amended statute of limitations could not be applied to cases where the statute of limitations period has already expired. This bill specifies that the amended statute of limitations applies to crimes committed on or after January 1, 2021.

5. Argument in Support

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

> Under existing law, the statute of limitations for most "white-collar" crimes (e.g. grand theft, identity theft, fraud, forgery, perjury, etc.) is four years after discovery or completion, whichever is later. (Pen. Code, § 801.5, 803(c).) Similarly, the statute of limitations for computer hacking is three years after discovery, if prosecuted civilly. (Pen. Code, §502(e)(5).) But the statute of limitations for felony computer hacking is three years from the date of the offense, which is inconsistent and counterintuitive. (Pen. Code, § 502(d)(1), 801.)
>
> As in "white-collar" crimes that involve deception or the exploitation of trust, victims of computer hacking are often not made aware of an electronic breach that results in the exfiltration or medication of data. Such crimes involving an anonymous online actor can take a long time to investigate following discovery of the offense in order to identity the perpetrator. For example, it was not until 2016 that Yahoo discovered that over a billion email accounts were compromised in 2013, which is beyond the statute of limitations.
>
> AB 1247 address this problem and harmonizes the law by permitting a complaint of felony computer hacking to be filed within 3 years after discovery or the commission of the offense, or within 3 years after the offense could have reasonably been discovered. In addition, the measure would establish an upper limit of 6 years from the date of the offense.

-- END –