
THIRD READING

Bill No: SB 922
Author: Chang (R), et al.
Amended: 6/18/20
Vote: 21

SENATE PUBLIC SAFETY COMMITTEE: 7-0, 5/20/20

AYES: Skinner, Moorlach, Bradford, Jackson, Mitchell, Morrell, Wiener

SENATE APPROPRIATIONS COMMITTEE: 7-0, 6/18/20

AYES: Portantino, Bates, Bradford, Hill, Jones, Leyva, Wieckowski

SUBJECT: Criminal procedure: limitations of actions

SOURCE: Conference of California Bar Associations

DIGEST: This bill amends the statute of limitations for felony offenses related to unlawful access of computer services and systems.

ANALYSIS:

Existing law:

- 1) 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.)
- 2) 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.)
- 3) 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).)

- 4) 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).)
- 5) 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).)
- 6) Provides that unless provided, as specified, a limitation of time is not tolled or extended for any reason. (Penal Code § 803, subd. (a).)
- 7) 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).)
- 8) States that, except as otherwise provided, prosecution for an offense is commenced when any of the following occurs:
 - a) An indictment or information is filed;
 - b) A complaint is filed charging a misdemeanor or infraction;
 - c) The defendant is arraigned on a complaint that charges the defendant with a felony; or,
 - d) 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.)
- 9) States that for purposes of determining the applicable limitation of time the following apply:
 - a) 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;
 - b) 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.)

- 10) 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;
- a) 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;
 - b) 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;
 - c) 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;
 - d) 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;
 - e) 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;
 - f) 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,
 - g) 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.)
- 11) Provides that a person who knowingly and without permission uses or causes to be used computer services shall be punished as follows:
- a) 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

- b) 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.*)
- 12) 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:
- a) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding \$1,000;
 - b) 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,
 - c) 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.*)
- 13) 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:
- a) 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,
 - b) 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.*)

- 14) 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:
 - a) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding \$1,000; or,
 - b) 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.*)
- 15) 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).)
- 16) 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:

- 1) Amends the statute of limitations for felony violations of unlawful access of computer services and systems which currently is three years after the commission of the offense to 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.
- 2) States 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

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.

FISCAL EFFECT: Appropriation: No Fiscal Com.: No Local: No

According to the Senate Appropriations Committee:

- State prison: Unknown, potential increase in state costs for new commitments to state prison that otherwise would not have resulted in incarceration. The FY 2020-2021 per capita cost to detain a person in a state prison is \$91,100 annually, with an annual marginal rate per person of over \$12,000. The actual costs would depend on how many defendants are sentenced to prison for a computer crime relevant to this measure after the current statute of limitations has lapsed. (General Fund)

- Court: Unknown, potentially-significant workload cost pressures to the court to adjudicate charges brought against defendants that would be time barred under current law. While the courts are not funded on a workload basis, an increase in workload could result in delayed court services and would put pressure on the General Fund to fund additional staff and resources. For example, the proposed 2020-21 budget would appropriate \$35.2 million from the General Fund to backfill continued reduction in fine and fee revenue for trial court operations. (General Fund*)

*Trial Court Trust Fund

SUPPORT: (Verified 6/18/20)

Conference of California Bar Associations (source)
Alameda County District Attorney
California District Attorneys Association
California Police Chiefs Association
California State Sheriffs' Association
Los Angeles County District Attorney's Office
National Insurance Crime Bureau
Peace Officers Research Association
Riverside Sheriffs' Association

OPPOSITION: (Verified 6/18/20)

None received

Prepared by: Stella Choe / PUB. S. /
6/23/20 17:13:38

**** END ****