
SENATE COMMITTEE ON PUBLIC SAFETY

Senator Loni Hancock, Chair

2015 - 2016 Regular

Bill No: AB 32 **Hearing Date:** July 7, 2015
Author: Waldron
Version: April 7, 2015
Urgency: No **Fiscal:** No
Consultant: JM

Subject: *Computer Crimes*

HISTORY

Source: Author

Prior Legislation: SB 1255 (Cannella) – Ch. 863, Stats. 2014
AB 1649 (Waldron) – Ch. 379, Statutes of 2014
SB 255 (Canella) – Ch. 466, Statutes of 2013

Support: Association of Deputy District Attorneys; Association for Los Angeles Deputy Sheriffs; California College and University Police Chiefs; California Communities United Institute; California District Attorneys Association; California Police Chiefs Association; Los Angeles Police Protective League; Riverside Sheriffs Association

Opposition: California Attorneys for Criminal Justice

Assembly Floor Vote: 78 - 0

PURPOSE

The purpose of this bill is to: 1) raise the maximum misdemeanor fines for computer access, use and damage crimes from \$5,000 to \$10,000; and 2) provide that the statute of limitations for any computer access, use or damage crime runs from the date of discovery if it is alleged that the defendant acquired, copied or distributed an image of sexual or intimate nature.

Existing law:

Defines numerous computer or electronic data offenses and imposes a wide range of penalties based on the seriousness of the offense or extent of harm caused by the defendant, including by a fine not exceeding \$10,000, by felony imprisonment pursuant to Penal Code Section 1170, subdivision (h) for a term of term of 16 months, two years or three years, or both, or by a fine not exceeding \$5,000, or by imprisonment in a county jail not exceeding one year. These penalties apply where any person knowingly:

- 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, 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 § 502, subs. (c) 1), (2), (4), (5), (10), (11), or (12); and (d)(1).)

Provides that any 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, by a fine not exceeding \$5,000, by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and
- For any violation that results in a victim expenditure in an amount more than \$5,000 or in an injury, if the value of the computer services used exceeds \$950, or for any second or subsequent violation, by a fine not exceeding \$10,000, by imprisonment pursuant to realignment for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding \$5,000, by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code § 502, subs. (c)(3); and (d)(2).)

Punishes any person who knowingly and without permission provides or assists in providing a means of accessing, accesses, or causes to be accessed a computer, computer system, or computer network as follows:

- A first violation that does not result in injury is an infraction punishable by a fine not exceeding \$1,000.
- Any violation that results in a victim expenditure in an amount not more than \$5,000, or for a second or subsequent violation, is a misdemeanor, punishable by a fine not exceeding \$5,000, by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment; and
- Any violation that results in a victim expenditure above \$5,000 is punishable by a fine not exceeding ten thousand dollars \$10,000, by felony imprisonment pursuant to Penal Code Section 1170, subdivision (h), for 16 months, two or three years, or both, or by a fine not exceeding \$5,000, by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code § 502, subs. (c) and (d)(3).)

Punishes any person who knowingly introduces any computer contaminant into any computer, or computer system, or computer network as follows:

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

- A violation that results in injury, or a subsequent violation, is punishable by a fine not exceeding \$10,000, by imprisonment in a county jail not exceeding one year, or by imprisonment pursuant Penal Code Section 1170, subdivision (h), or both that fine and imprisonment. (Pen. Code § 502 subds. (c)(14) and (d)(4).)

Punishes any person who knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network as follows:

- For a first violation that does not result in injury, an infraction punishable by a fine not more than \$1,000; and
- 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, subds. (c)(9) and (d)(5).)

Requires that prosecution for a felony - an offense punishable by imprisonment in the state prison or county jail pursuant to Penal Code Section 1170, subdivision (h) - be commenced within three years after commission of the offense, except as specified. (Penal Code, § 801.)

Requires that prosecution for an offense punishable by imprisonment in the state prison or county jail pursuant to realignment be commenced within three years after commission of the offense, except as specified. (Penal Code, § 801.)

States that, unless specified, prosecution for an offense not punishable by death or imprisonment in state prison shall be commenced within one year after commission of the offense. (Penal Code § 802.)

Provides that the statute of limitations for identity theft (Pen. Code § 530.5) or procuring or offering false instruments to be filed in a public officer (Pen. Code § 115) does not commence to run until the discovery of the offense. (Pen. Code § 803.5.)

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

Provides that if more than 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).)

This bill:

Increases the maximum fines from \$5,000 to \$10,000 in the misdemeanor crimes described above in “Existing law” involving computer and computer system access, use, disruption, damage or alteration, unless the current misdemeanor fine is \$10,000.

Provides where it is alleged that in the commission of a computer access, use, damage or alteration crime (Pen. Code § 502), the defendant acquired, copied, or distributed at least one digital image that displays a person’s intimate body part, the statute of limitations does not begin

to run until the discovery of the crime involving access, use, disruption, damage or alteration to or of a computer or computer system.

Provides the following definitions for the purpose of this special statute tolling the statute of limitations until the crime is discovered

- “Intimate body part” means any portion of the genitals, the anus, and in the case of a female also includes any portion of the breasts below the top of the areola, that is either uncovered or clearly visible through clothing; and
- “Digital images of a person” do not include representational images, artwork, or cartoon drawings.

RECEIVERSHIP/OVERCROWDING CRISIS AGGRAVATION

For the past eight years, this Committee has scrutinized legislation referred to its jurisdiction for any potential impact on prison overcrowding. Mindful of the United States Supreme Court ruling and federal court orders relating to the state’s ability to provide a constitutional level of health care to its inmate population and the related issue of prison overcrowding, this Committee has applied its “ROCA” policy as a content-neutral, provisional measure necessary to ensure that the Legislature does not erode progress in reducing prison overcrowding.

On February 10, 2014, the federal court ordered California to reduce its in-state adult institution population to 137.5% of design capacity by February 28, 2016, as follows:

- 143% of design bed capacity by June 30, 2014;
- 141.5% of design bed capacity by February 28, 2015; and,
- 137.5% of design bed capacity by February 28, 2016.

In February of this year the administration reported that as “of February 11, 2015, 112,993 inmates were housed in the State’s 34 adult institutions, which amounts to 136.6% of design bed capacity, and 8,828 inmates were housed in out-of-state facilities. This current population is now below the court-ordered reduction to 137.5% of design bed capacity.”(Defendants’ February 2015 Status Report In Response To February 10, 2014 Order, 2:90-cv-00520 KJM DAD PC, 3-Judge Court, *Coleman v. Brown, Plata v. Brown* (fn. omitted).

While significant gains have been made in reducing the prison population, the state now must stabilize these advances and demonstrate to the federal court that California has in place the “durable solution” to prison overcrowding “consistently demanded” by the court. (Opinion Re: Order Granting in Part and Denying in Part Defendants’ Request For Extension of December 31, 2013 Deadline, NO. 2:90-cv-0520 LKK DAD (PC), 3-Judge Court, *Coleman v. Brown, Plata v. Brown* (2-10-14). The Committee’s consideration of bills that may impact the prison population therefore will be informed by the following questions:

- Whether a proposal erodes a measure which has contributed to reducing the prison population;
- Whether a proposal addresses a major area of public safety or criminal activity for which there is no other reasonable, appropriate remedy;

- Whether a proposal addresses a crime which is directly dangerous to the physical safety of others for which there is no other reasonably appropriate sanction;
- Whether a proposal corrects a constitutional problem or legislative drafting error; and
- Whether a proposal proposes penalties which are proportionate, and cannot be achieved through any other reasonably appropriate remedy.

COMMENTS

1. Need for This Bill

According to the author:

Recent media has highlighted the increasing number of computer crimes that involve stealing intimate photos and also publishing them on the internet which emphasizes the public’s vulnerability to this kind of exploitation. Conventional computer hacking penalties do not sufficiently capture the emotional trauma that crimes including acquiring, copying, or distributing unauthorized intimate images can cause. AB 32 will make such crimes punishable by a fine of up to \$10,000 per image. The bill will establish that a person who commits such offense will not be able to evade prosecution by delaying release of the stolen images. AB 32 will also allow for a criminal prosecution within one year of when the crime was discovered. It is important to keep up with the new emerging computer crimes to make sure that the violators do not go unpunished and to prevent future crimes in such circumstances.

2. Penalty Assessments Effectively Quadruple any Criminal Fine

With very limited exceptions, all criminal fines are subject to “penalty assessments” that effectively quadruple the amount the defendant must actually pay. Simply put, if a criminal statute provides that the fine for the offense is \$100, the defendant will pay more than \$400. The court cannot relieve a defendant of the obligation to pay penalty assessments. Further, a defendant in every criminal case must pay a restitution fine that is deposited into the Restitution Fund that is used to reimburse victims of violent crime for specified expenses. The restitution fine for a misdemeanor is from \$150 to \$1,000. The fine for a felony is \$300 to \$10,000. The court cannot relieve a defendant of the obligation to pay a restitution fine.

The following chart breaks down the distribution of a Base Fine (the Fine stated in the Statute) and Penalty Assessments

| | |
|---|-------------|
| Base Fine: | \$10,000.00 |
| Penal Code § 1464 assessment (\$10 for every \$10): | \$10,000.00 |
| Penal Code § 1465.7 assessment (20% surcharge): | \$2,000.00 |
| Penal Code § 1465.8 assessment (\$40 per criminal offense): | \$40.00 |

| | |
|--|-------------|
| Government Code § 70372 assessment (\$5 for every \$10): | \$5,000.00 |
| Government Code § 70373 assessment (\$30 for felony or misdemeanor offense): | \$30.00 |
| Government Code § 76000 assessment (\$7 for every \$10): | \$7,000.00 |
| Government Code § 76000.5 assessment (\$2 for every \$10): | \$2,000.00 |
| Government Code § 76104.6 assessment (\$1 for every \$10): | \$1,000.00 |
| Government Code § 76104.7 assessment (\$4 for every \$10): | \$4,000.00 |
| <hr/> | |
| Fine with Assessments: | \$41,070.00 |
| <hr/> | |

Other fees and costs apply, including reimbursement to the county for court-appointed counsel. Large criminal fines may be difficult to collect, as collection could take years of effort and expense. The estimated amount of uncollected court ordered debt in 2011 was \$10.2 billion.¹

3. Confusing Fine Structure in This Bill and Existing Law

The purpose of this bill is to increase the maximum misdemeanor fines for unauthorized use or alteration of, or unauthorized access or damage to a computer or computer services from \$5,000 to \$10,000. The existing fine structure is unusual and confusing. The following is a representative example:

(C) 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 ten 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)(C).)

This appears to describe an alternate felony-misdemeanor (wobbler) in two ways: 1) by including two separate maximum fines (\$10,000 or \$5,000) as stand-alone penalties, and 2) providing that the court can sentence the defendant to a felony sentence pursuant to Penal Code 1170, subdivision (h) or impose a misdemeanor jail term of up to a year.

Penal Code Section 17, subdivision (b). defines an alternate felony-misdemeanor, or wobbler. In relevant part, Section 17 provides:

(b) When a crime is *punishable*, in the discretion of the court, *either by imprisonment in the state prison or imprisonment in a county jail under the provisions of subdivision (h) of Section 1170, or by fine or imprisonment in the*

¹ <http://www.lao.ca.gov/reports/2014/criminal-justice/debt-collection/court-ordered-debt-collection-111014.pdf>

county jail, it is a misdemeanor for all purposes under the following circumstances:

- (1) After a judgment imposing a punishment other than imprisonment in the state prison or imprisonment in a county jail under the provisions of subdivision (h) of Section 1170.

Applying Penal Code Section 17, subdivision (b), to the computer crimes covered by this bill, the sentencing court could impose a fine of up to \$10,000, with no felony jail or prison term and the offense would, by definition, be a misdemeanor. The court could impose a felony jail or prison sentence and no fine, and the offense would be a felony. The court could impose a felony jail or prison term and a fine of up to \$10,000 and the offense would be a felony. Simply stating that a crime is a felony punishable pursuant to Section 1170, subdivision (h), means that the defendant is subject to a sentence of 16 months, two years or three years *and* a fine of up to \$10,000. There is thus no need to specify that the maximum felony fine for a violation of Section 502 is \$10,000.

It is most likely that an appellate court would find that the maximum fine for a misdemeanor under existing law \$5,000, as the misdemeanor jail term is described in conjunction with a fine of up to \$5,000. However, it can also be argued that the court could impose a fine of up to \$10,000 and a misdemeanor jail term. As noted above, if a crime is punishable by a fine alone, it is a wobbler. If the court punishes the defendant by a county jail term, but not pursuant to Section 1170, subdivision (h), the offense is a misdemeanor. If the court can impose a fine of up to \$10,000 and county jail term, the bill is not necessary. If the court cannot impose a fine of up to \$10,000 and a misdemeanor jail term under existing law, the author's intent can be realized by simply striking the reference in the existing statutes to a \$5,000 fine. That would provide that the maximum fine for either a misdemeanor or a felony is \$10,000.

Committee staff has found no appellate cases discussing the fine structure in Penal Code Section 502. In any event, the penalty provisions in Penal Code Section 502 is confusing and should be clarified.

4. The Statute of Limitations Generally; Law Revision Commission Report

The statute of limitations requires 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. (Pen. 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.²

5. The Statute of Limitations Exception in this Bill

This bill extends the statute of limitation in prosecutions under Penal Code Section 502, subdivision (c). That subdivision is very broad. It includes many separate crimes for accessing, harming or using a computer, computer system or data in the computer or computer system. Specifically, the bill extends the statute of limitations if it is alleged that the defendant, in committing one of these crimes, “acquired, copied or distributed” a digital image in which an intimate - sexual - body part is displayed.

The bill does not require that the intimate image itself be illegal or that it be used in the commission of a crime. There is no requirement that the image be of an identifiable person. It can be argued that the image need not include a person’s face. The image could be in the public domain or previously and intentionally distributed by the person depicted. It also appears that the defendant need not even know that he or she “acquired, copied or distributed” an image of an intimate body part.

Further, it is not clear when or why a prosecutor would allege that a person “acquired, copied or distributed” an intimate or sexual image in the commission of a computer or compute system offense. Generally, prosecutor’s charge a crime and allege facts that support an enhancements or a sentencing limit or requirement. Acquiring, copying or distributing a sexual image is not an element of, or inherent in, any of the crimes in subdivision (c) of Section 502, although that conduct might be an element or inherently part of another crime, such as cyber porn revenge, or surreptitious filming of a person in a place where the person has a reasonable expectation of privacy.

The bill thus extends the statute of limitations for a crime because of a fact that is not directly related to the crime. The bill could extend the statute of limitations for one defendant, but not for another charged with the same crime, based on factors that could be essentially random or accidental, or extraneous to the offense. There are statutes of limitations that are based on factors that are not elements of the crime or inherent in the crime. However, those factors generally concern the fact that the victim was a minor at the time a sex crime occurred. While it appears that the statute is extended for crimes that do not include an element that the victim was a minor, sexual conduct with a minor is criminal and the age of the victim would typically be an element of a crime that is included in a greater offense, such as forced oral copulation.

² 1 Witkin Cal. Crim. Law Defenses, Section 214 (3rd Ed. 2004), citing 17 Cal. Law Rev. Com. Reports, pp.308-314.

Arguably, tolling of the statute of limitations for a computer crime based on the fact that the defendant “acquired, copied or distributed” an intimate digital image should also include a requirement that the acquisition, copying or distribution of the images constitutes criminal conduct, or at least an element of a crime.

6. Tolling the Statute of Limitation in Cases of Identity Theft - Application to Computer Hacking to Obtain Intimate Images of Another Person

It appears that many instances of the use of another person’s image - especially where the image was stolen from the depicted person’s computer - would constitute identity theft. Identity theft is a very broadly defined offense. It is essentially the unauthorized use of another person’s identifying information for any unlawful purpose. Identifying information is defined very broadly as well, including name, address, place of employment, biometric data, mother’s maiden name and many others. It appears that the unlawful purpose need not be a crime itself. The statute of limitations for identity theft does not begin to run until the crime has been discovered. In many situations where it appears that the author intends the statute of limitations in the bill to apply, the tolling provisions applicable to identity theft would apply.

The most infamous purveyor of non-consensual personal sexual images on the Internet is Hunter Moore. Moore ran a website on which he and others posted nude photos that were often described as “revenge porn,” because posters were often men eager to humiliate former partners. Moore went far beyond simply posting images provided to him by others. He employed a man named Charles Evens to hack into e-mail accounts to obtain the images. Moore and Evens recently pleaded guilty in federal court to computer hacking crimes and identity theft.³

In addition to hacking issues, using the images of actors and other celebrities can constitute a violation of a celebrity’s copyright or publicity rights. Under California law an actor, singer or other celebrity generally has a right to control and gain from the commercial value of his or her image, voice and other characteristics. (Cal. Civ. Code § 3344.1.) Unauthorized use of a celebrity’s image could perhaps be the basis of an identity theft prosecution.

7. Prior Legislation

AB 1649 (Waldron) - Ch. 379, Stats. of 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, and changed and added the definition of specified terms.

SB 255 (Cannella) - Ch. 466, Stats. of 2013 and SB 1255 (Cannella) - Ch. 863, Stats. of 2014 created and expanded a new misdemeanor for the distribution of a sexual or intimate image of an identifiable person where the distributor and the person depicted have agreed the images shall remain private. The offense includes the elements of serious emotional distress to the depicted person, which the distributor knew or should have known would have occurred.

-- END --

³ <http://www.nytimes.com/aponline/2015/02/18/us/ap-us-revenge-porn.html>