SENATE COMMITTEE ON PUBLIC SAFETY

Senator Loni Hancock, Chair
2015 - 2016 Regular

Bill No:	SB 1137	**Hearing Date:**	April 12, 2016
Author:	Hertzberg		
Version:	March 31, 2016		
Urgency:	No	**Fiscal:**	Yes
Consultant:	JM		

Subject: ***Computer Crimes: Ransomware***

HISTORY

Source: TechNet; Los Angeles County District Attorney

Prior Legislation: AB 32 (Waldron) Ch. 614 Stats. 2015
AB 1649 (Waldron) – Ch. 379, Statutes of 2014

Support: Association of Orange County Deputy Sheriffs; California Association of Licensed Investigators; California Police Chiefs Association; California State Sheriffs' Association; California Statewide Law Enforcement Association; Fraternal Order of Police, California State Lodge; Long Beach Police Officers Association; Sacramento County Deputy Sheriffs' Association

Opposition: Legal Services for Prisoners with Children

PURPOSE

The purpose of this bill is to: 1) separately define as a felony the crime of placing a contaminant or lock on a computer or computer system for the purpose of locking or controlling the computer, computer system or data files, coupled with a demand for payment of money or other consideration before the lock will be removed of control returned to owner or authorized user; and, 2) to specifically define such a contaminant or lock as "ransomware."

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 by felony imprisonment pursuant to Penal Code Section 1170, subdivision (h) for a term of term of 16 months, two years or three years and a fine of up to $10,000, or as misdemeanor by a fine not exceeding $5,000, or a fine of up to $1,000 by imprisonment in a county jail not exceeding one year, or as infraction. (Pen. Code § 502.) 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
- 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
- Introduces any computer contaminant into any computer, or computer system, or computer network as follows:
- 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:. (Pen. Code § 502, subds. (c)(9) and (d)(5).)

Existing law defines extortion as the obtaining of property from another person, without the person's consent, or obtaining an official act of a public officer, induced by the wrongful use of force or fear, or under color of official right. (Pen. Code § 518.)

Existing law defines force or fear sufficient to commit extortion as a threat to do any of the following:

- Injure the person or property of the person threatened or a third person.
- Accuse the threatened person or a relative of a crime.
- Expose or impute to the person threatened or a relative any deformity, disgrace or crime.
- Expose any secret of the person or relative.
- To report the immigration status of the person or a relative (Pen. Code § 519.)

Existing law provides that extortion is a felony, punishable pursuant to Penal Code Section 1170, subdivision (h), to an executed felony sentence of two, three or four years. (Pen. Code § 520.)

Existing law provides that *attempted* extortion is an alternate felony-misdemeanor, punishable by a jail term of up to one year, a fine of up to $1,000, or both, or by a *prison* term of 16 months, two years or three years and a fine of up to $10,000.

Existing law includes "white collar" financial crime prison sentence enhancements of 1-5 years and special fines, depending on the amount of money or property taken by the defendant or the loss suffered by the victim. The enhancements apply where the defendant is convicted of two or more related felonies and the loss to the victim or gain to the defendant is at least $100,000. To prevent a defendant from secreting or dissipating his or her assets, the court may order pretrial seizure of assets to preserve them for restitution and fines. (Pen. Code § 186.11.)

Existing federal law includes the Computer Fraud and Abuse Act ("CFAA"), which prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data. (18 U.S.C. § 1030(a)(1)-(7)).

Existing federal law provides that a person who intends to extort from any person any money or other thing of value and transmits in interstate or foreign commerce any communication containing either of the following:

- A threat to damage a protected computer;
- A threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
- A demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion." A first violation is punishable by imprisonment for up to five years and a fine determined pursuant to the sentencing guidelines.[1] A violation that follows conviction for this offense or a related offense is punishable by imprisonment for up to 10 years and a fine determined through the sentencing guidelines. (18 U.S.C. § 1030 (a)(7).)

  This bill provides that the person responsible for placing "ransomware" on a computer, computer system, or data in a computer system is a felony, punishable pursuant to Penal Code Section 1170, subdivision (h), by an executed felony sentence of two years, three years or four years and a fine of up to $10,000.

  This bill with defines "ransomware" as the placement or introduction of a computer contaminant or lock on a computer, computer system, or data in a computer system, coupled with a demand that money or other consideration be paid to the person responsible for the contaminant or lock before it is removed or repaired.

  This bill provides that one is responsible for ransomware if the person directly places or introduces the contaminant or lock, or directs or induces another person to do so, with the intent to demand payment or other consideration to remove the contaminant, unlock the computer system or data, or repair the computer, computer system or data.

RECEIVERSHIP/OVERCROWDING CRISIS AGGRAVATION

For the past several 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.

[1] It appears that the fine would be no more than $250,000 or twice the gain or loss in the crime. (18 U.S.C. § 3571.)

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 December of 2015 the administration reported that as "of December 9, 2015, 112,510 inmates were housed in the State's 34 adult institutions, which amounts to 136.0% of design bed capacity, and 5,264 inmates were housed in out-of-state facilities. The current population is 1,212 inmates below the final court-ordered population benchmark of 137.5% of design bed capacity, and has been under that benchmark since February 2015." (Defendants' December 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).) One year ago, 115,826 inmates were housed in the State's 34 adult institutions, which amounted to 140.0% of design bed capacity, and 8,864 inmates were housed in out-of-state facilities. (Defendants' December 2014 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 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:

> Kidnapping and ransom demands have been around as long as criminal activity itself. But what is new in the digital age is the immediacy in which a computer hacker can access and hold your computer hostage. Computer users are told that the only way to get their machines back is to pay a steep fine. This is known as "ransomware," a computer virus that renders files unobtainable until a ransom is paid.

> Essentially online extortion, ransomware involves infecting a user's computer with a virus that locks it. The attackers demand money before the computer will be unlocked, but once the money is paid attackers may not unlock the system. One of the scarier things about ransomware is that criminals can use victims' machines however they like. While the computer is locked, the criminals can steal passwords and even get into the victim's online bank accounts. Ransomware affects victims financially and imposes additional costs of replacing breached hardware, bringing legal action, and updating system security.
>
> This doesn't just impact home computers. Businesses, financial institutions, government agencies, academic institutions, and other organizations can and have become infected as well, resulting in loss of sensitive or proprietary information, disruption of regular operations, financial losses incurred to restore systems and files, and/or potential harm to an organization's reputation. In 2014, according to a recent report, 43 percent of companies experienced some sort of data breach, including highly visible and damaging attacks on Sony, Home Depot, Target and JP Morgan Chase.
>
> This bill defines "ransomware" in state law and makes it a crime to introduce ransomware into any computer, system, or network. The range of punishment (up to four years imprisonment) is equivalent to the punishment under current law for extortion.

2. Using Ransomware is Criminal under Existing California and Federal Laws, including Extortion and Introducing a Contaminant into a Computer or Computer System

The use of ransomware to demand a payment from a computer or computer system owner or operator appears to constitute extortion under existing California law. California law (Pen. Code § 502 – the section amended by this bill) also makes it a crime to access, damage or alter a computer system or data without permission. Section 502 specifically lists prohibited acts and provides various penalties, based on the severity of the harm caused or value of services taken.

This bill would add the use of ransomware as a computer crime in Section 502. The penalty for this form of computer crimes is the same as the penalty for extortion, a felony term of two, three, or four years. (Pen. Code § 518-527.) A prosecutor could charge ransomware with the very specific crime defined by this bill and the more general crime of extortion. A prosecutor could perhaps conclude that jurors would have a set understanding of extortion as meaning a demand for protection money from a store owner or blackmail to hide an embarrassing secret that they might be confused or reluctant to apply extortion to a highly technical and sophisticated computer scheme. A defendant, however, convicted of both offenses would be subject to a single punishment. California sentencing law generally permits a prosecutor to obtain a conviction on every crime covered by the defendant's conduct. However, the defendant can only be punished a single time for one act that violates a number of criminal statutes or for multiple offenses committed in one indivisible transaction. (Pen. Code § 654.)

3. Explosion in Computer and Data Fraud and Extortion Incidents and Awareness

It appears that the use of ransom to extort money or other form of exchange, such as bitcoin, has become nearly ubiquitous. Even relatively large-scale attacks on or seizure of control over computers, computer systems and computer can be done quickly and remotely.

Victims can reasonably conclude that they have little option but to comply. The perpetrators might well be in another country or even another continent. An attempt to obtain assistance from law enforcement may be futile and the perpetrators could punish such attempts by destroying data that includes an entity's entire operation. A business or organization could conclude that it could no longer function if the threat is carried out. Even where the threat is not executed, the very admission of the event could be extremely harmful to a business or other organization's reputation. For example, a hospital would be loath to admit that confidential medical records were seized or locked. The customers and clients of banks and brokerage houses must believe that their financial holdings and information are safe. Attorneys cannot afford to reveal the confidences of clients stored in digital files.

Computer criminals have become increasingly sophisticated as technology became more sophisticated and essential to the life of virtually every person and entity. The attacks have included locking or encrypting files on the home computers of individual victims – often through authentic-look law enforcement notifications that the victim has done some wrong that he or she would never want exposed.[2] The attacks have also included attacks on large entities, such as three hospitals in recent, well-publicized incidents in Southern California[3] and government entities. It appears that no media report of ransomware incidents is complete without noting that even police departments have paid ransoms to computer criminals. A February 20, 2015 story in the Chicago Tribune reported the suburban Chicago town of Midlothian paid a hacker $500[4] in bitcoin for release of infected files. Even the department's backup files were encrypted.

A number of computer, software and computer and computer data security businesses have developed products to detect and remove ransomware. Numerous on-line guides about ransomware have been published. These typically include descriptions of ransomware, how to detect ransomware, remove it and protect against. For example, the Mountain View, California firm Symantec has published particularly detailed guides[5] for addressing ransomware questions, concerns, protection, removal and repair.[6] TechNet – a Microsoft division that is a co-sponsor of this bill also publishes detailed ransomware guides and assistance, including information about newly discovered ransomware.[7]

Comparison with Identity Theft

In recent decades, identity theft has become a growing and daunting crime problem. Traditional investigative techniques did not work well to combat identity theft, a crime that was often committed by unseen, electronic means, creating law enforcement problems similar to recent ransomware incidents.

---

[2] https://www.fbi.gov/news/stories/2012/august/new-internet-scam
[3] http://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal-hospitals-ransomware-20160322-story.html
[4] http://www.chicagotribune.com/news/local/breaking/ct-midlothian-hacker-ransom-met-20150220-story.html
[5] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
[6] http://www.symantec.com/tv/products/details.jsp?vid=1954285164001
[7] https://blogs.technet.microsoft.com/mmpc/2015/08/09/emerging-ransomware-troldesh/

In 1997, California was one of the first states to create a crime specifically described as identity theft in Penal Code section 530.5.[8] Prior to that time, law enforcement agencies generally considered the defrauded business entity that was defrauded to be the victim of identity theft, not the person whose identity was stolen so that the fraud could be committed, although applicable statutes described a person whose identity was misused as a crime victim. However, advocates believed that the person who was the actual victim often found himself or herself given no respect or standing in repairing the damage done by the crime.

It would appear that the greatest value in the current identity theft statutes is to allow a victim to clear his or her name. Penal Code section 530.6 allows an identity theft victim to require the police to investigate an identity theft report and further allows the victim to use the report to obtain a court order declaring that he or she did not commit certain crimes or accumulate certain debts. Pursuant to this judicial procedure, a person may be listed in a database of identity theft victims maintained by the Department of Justice.

One of the most daunting and frustrating problems encountered by identify theft victims is the damage to one's credit. Good credit is essential to financial stability. An identity theft victim may well face months of work and substantial expense repairing his or credit. Companies marketing credit repair services. Credit card companies compete for business, in part, by including credit monitoring and repair in a credit account. Similar daunting problems face victims of ransomware and cryptoware. Business and government entities that were hacked must repair systems, recreate files and rebuild the trust of customers and citizens.

-- END –

[8] AB 156 (Murray) Ch. 768, Stats. 1997