SENATE COMMITTEE ON PUBLIC SAFETY

Senator Steven Bradford, Chair
2021 - 2022 Regular

Bill No:	AB 1391	**Hearing Date:**	June 29, 2021
Author:	Chau		
Version:	June 24, 2021		
Urgency:	No	**Fiscal:**	No
Consultant:	MK		

Subject: ***Unlawfully obtained data***

HISTORY

Source: Author

Support: California Health Coalition Advocacy

Opposition: California Chamber of Commerce (unless amended)

Assembly Floor Vote: 78 - 0

SEE COMMENT #7 FOR AMENDMENTS AFTER TESTIMONY WAS TAKEN

PURPOSE

The purpose of this bill is to prohibit the sale of data or sale of access to data, as defined, that a person has obtained pursuant to the commission of a crime, and would prohibit the purchase or use of data from a source known to have obtained or accessed that data pursuant to the commission of a crime.

Existing law pursuant to the federal Computer Fraud and Abuse Act of 1986, criminalizes several acts pertaining to computer access or use that is unauthorized or exceeds authorization, including, among other things, knowingly and with the intent to defraud, trafficking in any password or similar information through which a computer may be accessed without authorization if such trafficking affects interstate or foreign commerce or such computer is used by or for the Government of the United States. (18 U.S.C. Section 1230.)

Existing law pursuant to federal law, prohibits the receipt, possession, concealment, storing, bartering, selling, or disposing of any goods, wares, or merchandize, securities, or money of the value of $5,000 or more, or pledges or accepts as security for a loan any goods, wares, or merchandise, or securities, of the value of $500 or more, which have crossed a State or United States boundary after being stolen, unlawfully converted, or taken, knowing the same to have been stolen, unlawfully converted, or taken. (18 U.S.C. Section 2315.)

Existing law, establishes the California Consumer Privacy Act of 2018 (CCPA), which gives consumers certain rights regarding their PI, as defined, such as: (1) the right to know what PI is collected and sold about them; (2) the right to request access to the specific PI the business has

retained about them; (3) the right to request the deletion of the PI that the business has collected about them; (4) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age; and (5) the right to pursue a cause of action against a business that has suffered a data breach in the event the consumer's PI has been impermissibly accessed. (Civil Code Sections 1798.100 et seq.)

Existing law provides that, except as specified, any person who knowingly and without permission commits any of the following acts is guilty of a public offense:

- accesses and alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either devise or execute a scheme to defraud, deceive, or extort, or to wrongfully control or obtain money, property, or data;
- accesses and takes, copies, or makes use of any data from a computer, computer system, or computer network;
- uses or causes to be used computer services;
- adds, alters, damages, deletes, or destroys any data, computer software, or computer programs;
- 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;
- provides or assists in providing a means of accessing a computer, computer system, or computer network to commit a prohibited act;
- accesses or causes to be accessed any computer, computer, computer system, or computer network;
- introduces any computer contaminant, as defined, into any computer, computer system, or computer network; or
- uses the internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more emails or posts, thereby damaging or causing damage to a computer, computer data, computer system, or computer network. (Penal Code Section 502(c).)

Existing law specifies that a person who commits an act in violation of the provisions of 3), above, shall be guilty of either a misdemeanor or felony, depending on the particular violation, and may be subject to fines and/or imprisonment, as specified based on the facts of the case. (Penal Code Section 502(d).)

Existing law, provides that, in addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of the provisions of 3), above, may bring a civil action against the violator for compensatory damages, including any expenditure incurred to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access, and injunctive or other equitable relief. (Penal Code Section 502(e).)

Existing law, defines "data" to mean a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions; and specifies that data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device. (Penal Code Section 502(b)(8).)

Existing law specifies that one who wrongfully detains a thing, or gains a thing by fraud, accident, mistake, undue influence, the violation of a trust, or other wrongful act is an involuntary trustee of the thing gained, for the benefit of the owner or person who otherwise would have had it. (Civil Code Sections 2223 and 2224.)

Existing law provides that all proceeds from the preparation for the purpose of sale, the sale of the rights to, or the sale of materials that include or are based on the story of a felony for which a convicted felon was convicted shall be subject to an involuntary trust for the benefit of the beneficiaries, as specified. (Civil Code Section 2225(b).)

Existing law permits a beneficiary, as defined, to bring an action against a convicted felon, representative of the felon, or profiteer of a felony to recover their interest in the trust established by 7) or 8), above, in accordance with specified procedures. (Civil Code Section 2225(c).)

This bill makes it unlawful for a person to sell data, or sell access to data, that the person has obtained or accessed pursuant to the commission of a crime.

This bill makes it unlawful for a person, who is not an authorized person, to purchase or use data from a source that the person knows or reasonably should know has obtained or accessed that data pursuant to the commission of a crime.

This bill defines "authorized person" to mean a person who has come to possess or access the data lawfully and who continues to maintain the legal authority to possess, access, or use that data, under state or federal law as applicable. "Data" has the same meaning as defined in Section 502 of the Penal Code.

This bill clarifies that it shall not be construed to limit the constitutional rights of the public, including those described in *Bartnicki v. Vopper* (2001) 532 U.S. 514.

This bill provides that liability thereunder does not limit or preclude liability under any other law.

COMMENTS

1. Need for This Bill

According to the author:

> Current law fails to protect hacking victims from their data being sold by third parties. Civil Code section 2224 technically affords hacking victims a civil legal remedy, such as a constructive trust, to claim the profits a hacker made from the stolen data. Further, in criminal court, a hacker may be ordered to compensate their victims in the form of restitution. While the remedies of constructive trust and restitution are effective tools for addressing victims' damages incurred from hackers,

the law still fails to address the selling, purchasing, or utilizing of hacked data by third parties. The law must be amended to make clear that disseminating hacked data is unlawful, regardless of whether a hacking victim may be compensated through a constructive trust or restitution.

2. Prohibition on Selling and Purchasing Hacked Data

The Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) reported over two million complaints of internet crime over the past five years, totaling over $13 billion dollars in resulting losses. The number of reported internet crimes has increased every year since 2016, as have the associated costs, and the margin by which these rates increase year-over-year continues to grow. Between 2019 and 2020 alone, the number of complaints received by the FBI IC3 increased by nearly 70%, from 467,361 in 2019 to 791,790 in 2020, likely as a result of unprecedented demand for virtual technologies resulting from the COVID-19 pandemic. According to the FBI IC3's 2020 report, California leads the nation in both the number of complaints relating to internet crime, and in the estimated costs experienced by the victims. In 2020, the FBI IC3 received 69,541 cybercrime complaints from Californians, costing victims over $620 million – over $200 million more than New York, the next closest state.[1]

There have been several high profile, large-scale data breaches resulting in troves of personal information (PI) and other data falling into the hands of malicious actors. For instance, in 2013, the records of over a billion users was compromised from the email system of Yahoo, including names, birth dates, phone numbers, passwords, backup email addresses, and security question answers.[2] More recently, a massive breach of Facebook's databases compromised the PI of over 533 million users from 106 countries, including over 32 million records on users in the U.S. These data included phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses.[3]

The motives of those purchasing compromised data vary, ranging from the use of more benign data to support future phishing attacks to direct attempts at identity theft, and there is even evidence that law enforcement has purchased hacked data to use for investigative purposes. .[4]

It is not clear whether the sale or purchase of hacked data is criminalized under Federal Law. Federal law criminalizes the sale and purchase of stolen merchandise exceeding a certain value, but whether data constitutes "goods, wares, or merchandise, securities, or money" for the purposes of that law remains an open question. (18 U.S.C. Sec. 2315.) Pursuant to the federal Computer Fraud and Abuse Act of 1986, existing law also criminalizes several acts pertaining to computer access or use that is unauthorized or exceeds authorization, including, among other things, knowingly and with the intent to defraud, trafficking in any password or similar information through which a computer may be accessed without authorization if such trafficking

---

[1] Internet Crime Complaint Center, "Internet Crime Report 2020," *Federal Bureau of Investigation*, March 2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics, [as of Mar. 28, 2021].

[2] Vindu Goel & Nicole Perlroth, "Hacked Yahoo Data Is for Sale on Dark Web," *The New York Times*, Dec. 15, 2016, https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html, [as of Apr. 6, 2021].

[3] Aaron Holmes, "533 million Facebook users' phone numbers and personal data have been leaked online," *Insider*, Apr. 3, 2021, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4, [as of Apr. 6, 2021].

[4] Joseph Cox, "Police Are Buying Access to Hacked Website Data," *Vice*, Jul. 8, 2020, https://www.vice.com/en/article/3azvey/police-buying-hacked-data-spycloud, [as of Apr. 6, 2021].

affects interstate or foreign commerce or such computer is used by or for the Government of the United States. (18 U.S.C. Sec. 1230.) Outside of those limited circumstances, however, and with respect to data that does not include account or computer access information, federal law is silent on the matter of purchasing or selling data obtained through unauthorized access. California state law, while criminalizing several acts of unauthorized computer access and use, does not explicitly prohibit the marketing of stolen data, limiting its applicable prohibition only to knowingly and without permission providing or assisting in providing a means of accessing a computer, computer system, or computer network to commit a prohibited act. (Penal Code Section 502(c)(13).) Thus, so long as the seller of the data did not also perpetrate the hack, they can profit from it with relative impunity.

This bill attempts to fill the gaps by making it clearly unlawful for a person to sell data, or sell access to data, that the person has obtained or accessed pursuant to the commission of a crime. This prohibition targets the conduct after the initial unauthorized access or use has been accomplished and gets at the financial motives for committing the initial crime.

The bill further provides that it is unlawful for a person, excluding authorized persons, to purchase or use data from a source that the person knows or reasonably should know has obtained or accessed that data pursuant to the commission of a crime. This provision ensures that downstream buyers or users are also held to account for improper use and receipt of stolen or otherwise unlawfully obtained data.

There are lawful companies that are hired to perform cybersecurity or keep an eye out for identity theft for individuals and may purchase data that they know may have been obtained illegally in order to perform these tasks. Does the author's recent amendment to modify the definition of authorized use to include the possession, access or use of data under state or federal law address concerns that this bill would make illegal such cybersecurity and identity theft activities.

3. First Amendment Concerns

Any time there is restrictions on the sharing of information by the Government, First Amendment concerns may arise.

In *New York Times Co. v. Sullivan* (1964) 376 U.S. 254, 269, the Supreme Court held: "The general proposition that freedom of expression upon public questions is secured by the First Amendment has long been settled by our decisions."

In *Bartnicki v. Vopper* (2001) 532 U.S. 514, 517, the United States Supreme Court was faced with "an important question concerning what degree of protection, if any, the First Amendment provides to speech that discloses the contents of an illegally intercepted communication." The case involved "the repeated intentional disclosure of an illegally intercepted cellular telephone conversation about a public issue. The persons who made the disclosures did not participate in the interception, but they did know -- or at least had reason to know -- that the interception was unlawful."[5] After citing the reasoning in *Sullivan*, the court concluded: "We think it clear that parallel reasoning requires the conclusion that a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern."[6]

---

[5] *Bartnicki v. Vopper* (2001) 532 U.S. 514, 517-518.

[6] *Id.* at 535.

In order to protect legitimate free speech, the bill provides that it shall not be interpreted to limit the constitutional rights of the public, including those detailed in *Bartnicki*, pertaining to the rights of whistleblowers and the press regarding matters of public concern.

Does the language in the bill adequately address the rights of the press? Are the press' rights limited to those listed in *Barnicki?* Is *Barnicki* the appropriate case to cite? If the intent to protect the rights of the press be clearer if the section read something like "This section shall not be construed to limit the constitutional rights of the public, whistleblowers, or the press including those described in…."?

4. Enforcement

This bill makes the behavior it is addressing "unlawful". It is unclear as to what the penalty for this unlawful behavior in the civil code is. Is it intended to be civil remedies only or is it intended to create some sort of criminal liability, since the intent is to fill the gaps in Federal and State criminal law. The author office suggests that the bill is likely enforceable through the Business & Professions Code's unfair competition laws. B&P section 17200 defines unfair competition as "any unlawful business act or practice." and thus the relief would be injunctive relief and civil penalties. Not clear how a lone hacker is an unfair business practice, but if this is the intent should it be clarified that this behavior shall be considered an unfair business practice so there is no confusion as to the remedies?

5. Argument in Support

California Health Coalition Advocacy supports this bill stating:

> We agree that AB 1391 is an effective first step in addressing the growth of the hacked data marketplace by making clear that no one can knowingly sell, purchase or utilize hacked data.
>
> We appreciate that AB 1391 would: "make it unlawful for a person to sell, purchase, or utilize data, as defined, that the person knows or reasonably should know is compromised data. Further, it clarifies that its enactment will not conflict with the constitutional rights of whistleblowers and the press."

6. Oppose unless amended

With a letter submitted prior to the June 24, 2021 amendments, the California Chamber of Commerce opposes this bill unless it is amended stating:

> **AB 1391 Prohibits Lawful Cybersecurity and Identity Theft Practices**
>
> **AB 1391** fails to provide a critical operational allowance for cybersecurity purposes as established in 6 U.S.C. §1501(4); or the ability to provide otherwise lawful identity theft protections for consumers. By failing to account for these lawful, legitimate uses for information**, AB 1391** increases the value of illegally obtained information while simultaneously jeopardizing the safety and security of consumers online.

AB 1391 Does Not Account for Existing State or Federal Law

Additionally, **AB 1391** as drafted should clarify that uses under state or federal law are lawful purposes. **AB 1391** makes it unlawful for anyone to use data from a source that they reasonably should have known was obtained pursuant to the commission of a crime unless they are an "authorized person." However, the definition of authorized person may not fully cover legal uses. Thus, **AB 1391** makes illegally obtained information virtually inaccessible to good actors and cybersecurity professionals. For this reason, it is critical for the bill to expand the definition of "authorized person" to include persons and entities who have the legal authority to possess, access, or use that data "under state or federal law" as applicable. The bill, as drafted, will prohibit current legitimate uses that fall outside the language of the bill but are otherwise lawful.

AB 1391 Increases the Market for Illegal Data by Prohibiting Businesses from Scanning the Internet for That Information.

Further, **AB 1391** would benefit from providing a more concrete criminal element to trigger the prohibitions in this bill. Without this, **AB 1391** applies so broadly that it denies businesses and good actors the means to protect users and identify stolen information online and across the dark web. Even scanning the internet for stolen information becomes illegal under **AB 1391** because the very information being scanned-for has a potentiality of being illegally obtained. Specifically, the ambiguity between what a business *should* have known and a general lack of clarity about the definition of "pursuant to" the commission of a crime only shrinks the amount of information that businesses will be allowed to scan under this bill, and increases the amount of data that good actors are prohibited from accessing. In this way, **AB 1391** prohibits businesses and good actors from engaging in legitimate conduct that protects consumer safety and security online, but inadvertently creates new protections for criminals and bad actors.

Often, businesses cannot properly evaluate whether data was at some point sourced by criminal means, and even then, the very purpose of cybersecurity is to seek and identify information that may have been obtained through illegal means. To try and resolve for these concerns, the language in §1724(c) of the bill should be narrowed to apply only to information that a business "knows" was obtained "through" the commission of a crime, as opposed to "pursuant to" the commission of a crime.

Accordingly, we must respectfully **OPPOSE AB 1391 (Chau) UNLESS AMENDED** to address these legitimate operational concerns.

7. Amendments following testimony taken

After testimony was taken on June 22, this bill was amended on June 24 as follows:

(c) It is unlawful for a person, who is not an authorized person, to purchase or use data from a source that the person knows or reasonably should know has obtained or accessed that data ***through*** ~~pursuant to~~ the commission of a crime.

(d) This section *(1)* shall not be construed to limit the constitutional rights of the public**,** ***the rights of whistleblowers, and the press regarding matters of public concern,*** **including*****, but not limited to,*** those described in Bartnicki v. Vopper, (2001) 532 U.S. 514~~, pertaining to the rights of whistleblowers and the press regarding matters of public concern~~*;*

(e*) This section does not limit providing or obtaining data in an otherwise lawful manner for the purpose of protecting a computer system or data stored in a computer system or protecting an individual from risk of identity theft.*

(f) The court in an action pursuant to this section may award equitable relief, including, but not limited to, an injunction, costs, and any other relief the court deems proper.

(*g)* Liability under this section shall not limit or preclude liability under any other law.

(h) A violation of this section shall not constitute a crime.

-- END –