SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 1391 (Chau)
Version: April 12, 2021
Hearing Date: June 8, 2021
Fiscal: No
Urgency: No
CK

SUBJECT

Unlawfully obtained data

DIGEST

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. It further 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.

EXECUTIVE SUMMARY

A vast majority of Californians engage in a wide range of activities online. Even before the pandemic forced many people to drastically shift their lives online, 70 percent of people in the state received financial services online, 39 percent telecommuted, 42 percent accessed sensitive health or insurance records online, and 39 percent communicated with doctors.[1] In addition, many companies have realized the financial benefits of collecting as much data on consumers as possible, tracking, storing, and selling the details of our everyday lives. Given the amount of activity online and the massive amount of data being collected and switching hands, concerns about data security have skyrocketed. In 2020 alone, estimates suggest that there were over 1000 data breaches resulting in the exposure of over 155 million records.[2]

---

[1] Niu Gao & Joseph Hayes, *California's Digital Divide* (February 2021) Public Policy Institute of California, https://www.ppic.org/publication/californias-digital-divide/ [as of May 23, 2021]. All further internet citations are current as of May 23, 2021.
[2] Joseph Johnson, *Cyber crime: number of breaches and records exposed 2005-2020* (March 3, 2021) Statista, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/#:~:text=In%202020%2C%20the%20number%20of,%2Dthan%2Dadequate%20information%20security.

The market for this unlawfully obtained data is lucrative. In fact, this bill was motivated by revelations that some companies are selling government agencies access to stolen data creating an "end-run around the usual legal processes."[3] In order to address concerns that existing state and federal law fails to adequately target the selling, buying, and utilization of improperly attained data, this bill makes it unlawful for a person to sell data, or access to data, criminally obtained or accessed, and to buy or use such data, as provided. This bill is author-sponsored. There is no support for the bill. The Electronic Frontier Foundation is in opposition. Should the bill pass this Committee it will then be referred to the Public Safety Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Imposes criminal liability on any person who commits specified "computer crimes," including the following conduct:
    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 and without permission accesses or causes to be accessed any computer, computer system, or computer network; or
    d) knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section. (Pen. Code § 502(c).)

2) Defines "data," for the above provision, as a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. 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. (Pen. Code § 502(b)(8).)

3) Authorizes the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a

[3] Joseph Cox, *Police Are Buying Access to Hacked Website Data* (July 8, 2020) Vice, https://www.vice.com/en/article/3azvey/police-buying-hacked-data-spycloud.

violation of any of the above provisions to bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. A court may also award reasonable attorney's fees and punitive damages. These remedies are in addition to any other available civil remedy. (Pen. Code § 502(e).)

4) Establishes the California Consumer Privacy Act (CCPA), as amended by Proposition 24 (2020), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

5) Authorizes, pursuant to the CCPA, any consumer whose nonencrypted and nonredacted personal information, as defined, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information to institute a civil action to recover statutory damages, as provided, or actual damages, whichever is greater; injunctive or declaratory relief; and any other relief the court deems proper. (Civ. Code § 1798.150.)

6) Subjects any provider of health care, a health care service plan, pharmaceutical company, or contractor, who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of written or electronic medical records, to damages in a civil action or an administrative fine, as specified. (Civ. Code Sec. 56.36.)

7) Imposes criminal liability, pursuant to the federal Computer Fraud and Abuse Act, for specified fraud and related activity in connection with computers, including:
    a) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined, willfully communicates, delivers, or transmits to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

b) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains certain financial information or information from a protected computer;
c) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States;
d) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and thereby furthers the intended fraud and obtains anything of value; or
e) knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization, as provided. (18 U.S.C. Sec. 1230.)

This bill:

1) 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.

2) 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.

3) 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, as applicable. "Data" has the same meaning as defined in Section 502 of the Penal Code.

4) 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.

5) Provides that liability thereunder does not limit or preclude liability under any other law.

COMMENTS

1. Stated intent of the bill

According to the author:

> Today, we live in a digitally connected world where more people have access to the internet than ever before. Further, amidst the pandemic, internet access has quickly become a basic necessity for all aspects of life.

However, as more people use computers and the internet, criminals have more opportunities to hack information. In the first half of 2019, data breaches exposed 4.1 billion records; yet in the first half of 2020, 36 billion records were exposed. These types of cybercrimes range from breaking into one's computer network to steal financial information to other crimes, such as corporate espionage, fraud, and extortion.

Current law criminalizes computer hacking and stealing information in all forms. Nevertheless, some companies have seized the opportunity to turn a profit by selling data originally obtained by hackers. For example, the news recently reported on a company that sells access to breached personal data, including to law enforcement. Nothing in law restricts such sales in any manner.

As a state that is home to some of the most comprehensive laws protecting electronic communications and where the right to privacy is enshrined in our Constitution, California should lead the way in stopping the rise of a hacked data marketplace.

This bill 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.

2. Combatting the market for illegally obtained data

a. Understanding the scope of the problem

As indicated above, data is a valuable commodity that is always at risk of unauthorized access whether through internal exfiltration or hacks enabled by insufficient security features. According to the Federal Bureau of Investigation's (FBI) Internet Crime Report, the Internet Crime Complaint Center received "a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019."[4] A brief look at a few of the larger breaches illustrates the scope of the problem.

The infamous breach at Equifax lasted at least several months in 2017. "If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies."[5] The hackers involved were able to access people's names, Social Security numbers, birth dates,

[4] Internet Crime Complaint Center, *2020 Internet Crime Report* (March 17, 2021) FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
[5] Seena Gressin, *The Equifax Data Breach: What to Do* (Sep. 9, 2017) Federal Trade Commission, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

addresses, and driver's license numbers. Over 200,000 consumers also had their credit card numbers stolen. There is evidence that the massive hack of personal information has led to extensive identity theft with the thieves using the stolen information to apply for mortgages, credit cards, and student loans. The information is also being used to tap into bank accounts, to file insurance claims, and to incur massive debts on behalf of affected consumers.

Even before that, a much larger breach occurred in 2013, when hackers accessed Yahoo's email system, gathering data on more than 1 billion users.[6] Several years after the hack, a group began offering the entire database of information for sale on the so-called "dark web," with at least three confirmed buyers paying $300,000 each. The breach was not disclosed by Yahoo until 3 years after it occurred. It came after an earlier breach of 450,000 accounts in 2012 and before a hack in 2014 of 500 million user accounts.

More recently, in 2019, the personal information of over 530 million Facebook users was taken in a breach that exploited a vulnerability in a Facebook feature.[7] The company recently indicated it has decided not to notify the individual users affected, but the information remains publicly available after being posted to an online hacking forum. Major breaches have also occurred in the last year, with GEICO having driver's license data on 132,000 customers stolen and a hack of the ParkMobile application resulting in the personal information of 21 million users exposed.[8]

b. Laws to combat not only the theft but the motive

Existing state and federal law provides some form of criminal and civil redress for the unlawful access and use of data, but there are gaps in fully addressing the issues and conduct that arise in the cases discussed above. The ultimate motive for many of these hacks is financial gain. And there is generally no shortage of buyers in the market for such illegally obtained data. As seen in the massive Yahoo breach, hackers were able to make sales on the dark web. This included sales to scammers who will likely use the information to engage in identity theft or to phish more valuable information as well as an entity that "appeared more interested in espionage." However, as noted, even law enforcement has participated in this market for illegally obtained data.

---

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

[7] Emma Bowman, *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users* (April 9, 2021) NPR, https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.

[8] Zack Whittaker, *Geico admits fraudsters stole customers' driver's license numbers for months* (April 19, 2021) TechCrunch, https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/; Joe Marusak, *If you find parking spots with this popular app, your data may have been stolen* (April 16, 2021) Charlotte Observer, https://www.charlotteobserver.com/news/local/article250666434.html.

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.

3. Concerns with the bill

Some concerns were raised in response to a previous version of the bill about the impact on the protections of the First Amendment of the United States Constitution. It is true that the United States Supreme Court has found the First Amendment protects even illegally obtained information under certain circumstances where the information is of public concern.

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."[9] 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."[10]

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.

---

[9] *Bartnicki v. Vopper* (2001) 532 U.S. 514, 517-518.
[10] *Id.* at 535.

The Electronic Frontier Foundation writes in opposition to the bill. It expresses concerns related to the bill's interplay with copyright laws, which can involve criminal penalties.

SUPPORT

None known

OPPOSITION

Electronic Frontier Foundation

RELATED LEGISLATION

Pending Legislation: AB 825 (Levine, 2021) includes genetic data in the definition of personal information applicable to California's Data Breach Notification Law as it applies to public agencies, businesses, and persons. This bill is currently pending referral in the Senate.

Prior Legislation: AB 1130 (Levine, Ch. 750, Stats. 2019) included biometric data and certain identification numbers in the definition of personal information for purposes of California's Data Breach Notification Laws and required businesses to maintain reasonable security procedures and practices to protect such information.

PRIOR VOTES:

Assembly Floor (Ayes 78, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)

****