Date of Hearing: April 8, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1391 (Chau) – As Introduced February 19, 2021

AS PROPOSED TO BE AMENDED

SUBJECT: Compromised data

SUMMARY: This bill, as it is proposed to be amended, would 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. Specifically, **this bill would**:

1) Provide that it is 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) Provide that it is unlawful for a 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) Specify that the prohibition in 2), above, shall not be construed to prohibit an authorized person, as defined, from purchasing or using data that has been accessed or obtained from them pursuant to the commission of a crime.

4) Specify that the provisions of the bill shall not be construed to limit the constitutional rights of the public, including those provided for in *Bartnicki v. Vopper* (532 U.S. 514 (2001)) pertaining to the rights of whistleblowers and the press regarding matters of public concern.

5) Specify that prosecution under the provisions of this bill shall not limit or preclude prosecution under any other provision of law.

EXISTING LAW:

1) 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. Sec. 1230.)

2) 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. Sec. 2315.)

3) Pursuant to state 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. (Civ. Code Sec. 1798.100 et seq.)

4) 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. (Pen. Code Sec. 502(c).)

5) 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. (Pen. Code Sec. 502(d).)

6) 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. (Pen. Code Sec. 502(e).)

7) For the purposes of 3), above, 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. (Pen. Code Sec. 502(b)(8).)

8) 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. (Civ. Code Secs. 2223 and 2224.)

9) 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. (Civ. Code Sec. 2225(b).)

10) 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. (Civ. Code Sec. 2225(c).)

FISCAL EFFECT: None. This bill has been keyed non-fiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of this bill**: This bill seeks to eliminate markets for and mitigate dissemination of compromised data by deeming it unlawful to sell data obtained or accessed pursuant to the commission of a crime, and unlawful to purchase or use data from a source known to have obtained or accessed that data pursuant to the commission of a crime. This bill is author sponsored.

2) **Author's statement**: According to the author:

> 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.
>
> 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.

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 has been accessed or obtained pursuant to the commission of a crime.

3) **Sale and purchase of hacked data**: As society's everyday reliance on technology grows, so too do the vulnerabilities to and costs associated with cybercrime. 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]

Among these unfortunately common cyber-incidents are 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 were 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]

In some cases, hackers perpetrating these breaches intend to use the information recovered to perpetrate fraud, but more often, their incentive lies in the sizable value of these databases on illicit markets. According to Andrew Komarov, the chief intelligence officer at InfoArmor, an Arizona cybersecurity firm, "[t]hree buyers – two known spammers and an entity that appeared more interested in espionage – paid about $300,000 each for a complete copy of the database" compromised from Yahoo. Others noted that hackers were actively trying to sell

---

[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].

the stolen Yahoo data for as much as $200,000, with going rates diminishing to the tens of thousands of dollars as the data become less valuable.[2] Similarly, the data lifted from Facebook allegedly sold initially for tens of thousands of dollars, and continued to circulate on illicit markets for lower prices until it was finally published online for free. The data were also made available earlier this year by way of a bot built to provide access to the database for a fee charged on a per use basis.[4]

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, but for the initial hackers themselves, the enormous value of these databases garner on the open market incentivizes the risky endeavor of perpetrating the hack. Notably, the market for such data is not limited to the shady, extralegal reaches of the "dark web." An exposé published by *Vice* revealed that breached data are increasingly purchased by law enforcement entities as an end-run around the usual legal processes for generating investigative leads by way of legal requests for data.[5] In many cases, such purchases are made through intermediary companies that specialize in obtaining hacked data circulating on the dark web, and selling those data to law enforcement. SpyCloud, for instance, is a business that provides tools to individuals and organizations to detect and obstruct account takeovers, but also provides law enforcement with access to the exposed information of other people. As the *Vice* article notes:

> By buying products from SpyCloud, law enforcement would also be obtaining access to hacked data on people who are not associated with any crimes – the vast majority of people affected by data breaches are not criminals – and would not need to follow the usual mechanisms of sending a legal request to a company to obtain user data. […]
>
> "Normally, if the police want to find out, say, what IP address is associated with a particular online account, they do have to serve legal process on the service provider. This is an end-run around the usual legal processes. We impose those requirements on law enforcement for good reason," [Riana Pfefferkorn, associate director of surveillance and cybersecurity at the Stanford Center for Internet and Society] said. […]
>
> Pfefferkorn said, "Using these pools of breached data in this way is ethically dubious but so obviously attractive – for malign purposes as well as good."[5]

Disconcerting as it may be, this practice of selling hacked data to the highest bidder, be they malicious fraudsters or law enforcement agencies, may be not be illegal under existing 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

---

[4] Hannah Knowles, "533 million Facebook users' phone numbers, personal information exposed online, report says," *The Washington Post*, Apr. 4, 2021, https://www.washingtonpost.com/business/2021/04/03/facebook-data-leak-insider/, [as of Apr. 6, 2021].
[5] 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].

trafficking 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, though prohibitive of several acts of unauthorized computer access and use, similarly fails to 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. (Pen. Code Sec. 502(c)(13).) This legal ambiguity allows a market for breached data to thrive, as it is difficult to hold a party accountable for benefiting from the dissemination or use of those data, regardless of whether the victims of the breach continue to be affected. This means so long as the seller of the data did not also perpetrate the hack, they can profit from it with relative impunity.

AB 1391 seeks to prohibit the sale, purchase, and use of data obtained pursuant to the commission of a crime in order to provide legal avenues for suppressing the growing market for compromised data.

4) **With proposed amendments, AB 1391 prohibits transactions for disseminating and acquiring hacked data, and resolves various stakeholder concerns**: As it is currently in print, AB 1391 provides that it is unlawful for a person to sell, purchase, or utilize data that the person knows or reasonably should know is compromised data, and defines "compromised data" to mean data, as defined in Section 502 of the Penal Code, that has been obtained or accessed pursuant to the commission of a crime.

   As it is proposed to be amended, AB 1391 effectively seeks to accomplish the same end, though the language has been reconfigured to resolve certain ambiguities and stakeholder concerns. As proposed to be amended, the bill would refer to "data," as defined in Section 502 of the Penal Code, rather than "compromised data," and would provide that: (1) it is 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; and (2) it is unlawful for a person, who is not an authorized person, as defined, 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. The bill would define "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. In effect, this language would prohibit the initial sale of the hacked data, and would further allow for prosecution of the purchaser of that data. Imposing such liability on the purchaser should reduce demand for the data, especially by legitimate entities, and would provide the tools to intervene in the continued dissemination of hacked data that would otherwise further victimize those whose data have been compromised.

5) **Proposed amendments**: The author has worked closely with stakeholders and Committee staff to craft amendments that clarify potential ambiguities and ensure that the bill would not impose on constitutional rights.

   - <u>Reconfiguring operative language to clarify a person's ability to purchase back or continue to use their own data that has been compromised</u>: Several industry stakeholders raised concerns that the language of the bill in print would seem to prevent a person's

continued use of, and ability to lawfully sell, their own data if those data have been otherwise compromised. In other words, if a data breach occurs but the data that were inappropriately accessed remain in the possession of the victim, those data should not be off limits to the victim for normal use. Furthermore, stakeholders indicated that it is not uncommon for a business that suffers a data breach to attempt to buy back their own compromised data, either to regain access in the event their own access was revoked, or to determine the extent of the data compromised so as to effectively notify those affected. To resolve these concerns, the Committee proposes the following amendment:

- On page 1, in line 2, strike out "section, "compromised data" means", strike out lines 3 and 4, and insert:

  "section:

  (1) "Authorized person" means 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.

  (2) "Data" has the same meaning as defined in Section 502 of the Penal Code"

- On page 2, in line 1, strike out "sell, purchase, or utilize data", strike out lines 2 and 3, and insert:

  "sell data or sell access to data that the person has obtained or accessed pursuant to the commission of a crime.

  (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 pursuant to the commission of a crime."

- Clarifying that the provisions of the bill do not limit constitutional rights related to the publication of matters of public concern: Stakeholders pointed out that the Supreme Court of the United States has provided that the First Amendment protects the publication of information obtained unlawfully if, on balance, that interest in publishing a matter of public importance outweighs the privacy concerns the law intends to protect. Specifically, in *Bartnicki v. Vopper* (2001) 532 U.S. 514, the Supreme Court held:

  > Our opinion in *New York Times Co. v. Sullivan* [376 U.S. 254 (1964)] reviewed many of the decisions that settled the "general proposition that freedom of expression upon public questions is secured by the First Amendment. […] 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.

  To ensure that, by prohibiting the sale, purchase, and use of compromised data, this bill does not impinge on the rights of whistleblowers and journalists to publish matters of public concern, or any other constitutional right, the Committee proposes the following amendment:

- On page 2, insert: ***"(d) This section shall not be construed to limit the constitutional rights of the public, including 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."***

- Clarifying that liability under this section is cumulative upon liability under any other law: The Committee proposes the following amendment:

  - On page 2, insert: ***"(e) Liability under this section shall not limit or preclude liability under any other law."***

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200