California State Assembly

PRIVACY AND CONSUMER PROTECTION

ED CHAU
CHAIR

AGENDA

Tuesday, January 14, 2020
1:30 p.m. -- State Capitol, Room 126

BILLS HEARD IN SIGN IN ORDER

1.	AB 499	Mayes	Personal information: social security numbers: state agencies.
2.	AB 699	Grayson	Credit services organizations.
3.	AB 904	Chau	Search warrants: tracking devices.

CONSENT CALENDAR

4.	AB 325	Ramos**	Self-service storage facilities.
5.	AB 1263	Low	Contracts: consumer services: consumer complaints.

** with amends

Date of Hearing: January 14, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 499 (Mayes) – As Amended April 11, 2019

SUBJECT: Personal information: social security numbers: state agencies

SUMMARY: This bill would prohibit a state agency from sending any outgoing mail that contains an individual's full social security number (SSN), unless federal law requires inclusion of the full SSN, and would require each state agency to report to the Legislature when and why it mails documents that contain individuals' full social security numbers. Specifically, **this bill would**:

1) Beginning January 1, 2023, prohibit a state agency from sending any outgoing mail that contains an individual's full SSN unless, under particular circumstances, federal law requires the inclusion of the full SSN.

2) Require each state agency, on or before September 1, 2020, to report to the Legislature when and why it mails documents that contain individuals' full SSNs.

3) Until January 1, 2024, require a state agency that, in its estimation, is unable to comply with the prohibition on mailing full SSNs to submit an annual corrective action plan to the Legislature until it complies with the above provisions.

4) Require a state agency that is not in compliance with the prohibition on mailing full SSNs to offer to provide appropriate identity theft prevention and mitigation services to any individual, at no cost to the individual, to whom it sent mail that contained the individual's full SSN, as specified.

EXISTING LAW:

1) Prohibits any state agency from sending any outgoing United States mail to an individual that contains personal information about that individual, including, but not limited to, the individual's SSN, telephone number, driver's license number, or credit card account number, unless that personal information is contained within sealed correspondence and cannot be viewed from the outside of that sealed correspondence. (Gov. Code Sec. 11019.7.)

2) Prohibits a person or entity from printing an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires the SSN to be on the document to be mailed. However, SSNs may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the SSN. (Civ. Code Sec. 1798.85(a)(5).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to protect California residents from identity theft by, among other things, prohibiting state agencies from sending any mail to an individual

containing their full SSN, unless a full SSN is required by federal law. This bill is author-sponsored.

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

> It goes without saying that an individual's Social Security Number is one of the most important pieces of information an individual should protect. This legislation follows a recommendation by the State Auditor after an investigation into the Employment Development Department (EDD) practice of sending out mail with full Social security numbers. EDD exposed nearly 300 claimants to the risk of identity theft when it inappropriately disclosed their personal information, including SSNs, to other mail recipients. EDD is currently undergoing a system modernization project, which will incorporate a unique identifier to replace SSNs. However, this will not be completed before 2024 and EDD will send approximately 70 million documents with SSNs during this period. It is also unclear that EDD needs to send SSNs through the mail as the State Auditor could not find any laws expressly requiring them to do so.

3) **Widespread use of SSNs makes the identifier an attractive target for identity thieves**: According to the Social Security Administration, the use of the SSN has expanded significantly since its inception in 1936. Created merely to keep track of the earnings history of U.S. workers for Social Security entitlement and benefit computation purposes, it is now used as a nearly universal identifier. Assigned at birth, the SSN enables government agencies to identify individuals in their records and allows businesses to track an individual's financial information. Unfortunately, this universality has led to abuse as the SSN is a key piece of information used to commit identity theft. The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. (Puckett, *The Story of the Social Security Number* Social Security Bulletin, Vol. 69, No. 2, 2009.)

   For decades, California residents have benefited from laws protecting SSNs from disclosure by the private sector and government agencies. By way of example, SB 458 (Peace, Ch. 685, Stats. 1998) prohibited state agencies from sending any correspondence to an individual that contains personal information about that individual (*e.g.*, social security number, driver's license number, telephone number, or credit card account number) unless the correspondence is sealed. Additionally, since 2002, California has restricted the use and display of SSNs by private actors (*see* SB 168 (Bowen, Ch. 720, Stats. 2001)) by prohibiting companies and persons from engaging in certain activities, such as:

   - posting or publicly displaying SSNs;
   - printing SSNs on cards required to access the company's products or services;
   - requiring people to transmit an SSN over the internet unless the connection is secure or the number is encrypted;
   - requiring people to log onto a website using an SSN without a password; or,
   - printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.

Yet despite states like California regulating the use and disclosure of SSNs, continues. In September 2005, the United States Government Accountability Office issued a report entitled, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain.* The report found that "SSN use is widespread. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and perform research and evaluations of their programs. Although some government agencies are taking steps to limit the use and display of SSNs, these numbers are still available in a variety of public records held by states, local jurisdictions, and courts[.]"

After widespread media coverage of California's Employment Development Department (EDD) printing full SSNs on correspondence to millions of Californians in 2015, EDD claimed it would begin to redact SSNs on 75 percent of all mailed documents. In a recent report regarding EDD's privacy protection practices when mailing documents to its customers, the State Auditor concluded that "[a]lthough EDD has undertaken efforts since 2015 to reduce the amount of mail it sends to claimants that include full SSNs, its efforts have been insufficient." Specifically, the State Auditor found that "EDD likely sent more than 17 million pieces of mail containing full Social Security numbers (SSNs) to a total of more than a million people in fiscal year 2017–18 [and that] several of the security incidents [...] reviewed from 2015 through 2018 showed that EDD exposed nearly 300 claimants to the risk of identity theft when it inappropriately disclosed their personal information, including SSNs, to other mail recipients." (The full report (hereinafter "Report") may be found online at <http://www.auditor.ca.gov/pdfs/reports/2018-129.pdf> [as of Jan. 7, 2020].)

Ultimately, the State Auditor found that EDD should take near-term measures to protect its claimants better, and made several recommendations to that effect. This bill would codify a number of those recommendations for all state agencies.

4) **Prohibits the mailing of full SSNs to individuals unless required by federal law**: This bill would prohibit, beginning January 1, 2023, a state agency from sending any outgoing US mail to an individual that contains the individual's full SSN, unless federal law requires the inclusion of a full SSN. This prohibition is taken directly from the State Auditor's report which provides that "[b]ecause other state agencies may mail full SSNs to Californians, and because this practice—regardless of the agency involved—exposes individuals to the risk of identity theft, the Legislature should amend state law to require all state agencies to develop and implement plans to stop mailing documents that contain full SSNs to individuals by no later than December 2022, unless federal law requires the inclusion of full SSNs." (*See* Report at p 22.)

A similar prohibition was contained in SB 447 (DeSaulnier, 2012), which was vetoed by Governor Brown who argued that this prohibition "would hinder the ability of state agencies to promptly and accurately provide information to run essential programs." Arguably, many factors have changed since Governor Brown vetoed that bill eight years ago, thereby justifying the reconsideration of this prohibition by the Legislature. For example, since 2012 many state agencies have updated their privacy practices and means of correspondence in ways that ensure full SSNs are no longer being mailed. Specifically, as more agencies have embraced "paperless" communication, mailing correspondence has become rarer. Additionally, some agencies now issue unique identifiers in lieu of using an SSN, as recommended by California's Office of Privacy Protection (OPP) as early as 2008. Further,

as discussed more below, this bill is distinct from SB 447 in that a delayed implementation date will give state agencies that are still using full SSNs in mailed correspondence time to sufficiently prepare to implement the new law.

5) **Delayed implementation combined with reporting requirements gives state agencies time to update privacy practices and seek statutory amendments if necessary:** Beginning on or before September of this year, this bill would require each state agency to report to the Legislature when and why it mails individuals' full SSNs. Further, this bill would require any agency that, in its estimation, cannot cease mailing full SSNs to individuals by January 1, 2023, to provide to the Legislature an annual correction plan until it can stop mailing full SSNs. Similar to the prohibition discussed in Comment 4 above, these requirements are based on recommendations by the State Auditor in the Report. Specifically, the Report provides:

> To ensure that state agencies sufficiently prepare to implement this new law, the Legislature should also require that, by September 2019, they submit to it a report that identifies the extent to which their departments mail any documents containing full SSNs to individuals. If any agency determines that it cannot reasonably meet the December 2022 deadline to stop including full SSNs on mailings to individuals, the Legislature should require that starting in January 2023, the agency submit to it and post on the agency's website an annual corrective action plan that contains, at a minimum, the following information:
>
> - The steps it has taken to stop including full SSNs on mailed documents.
> - The number of documents from which it has successfully removed full SSNs and the approximate mailing volume that corresponds to those documents.
> - The remaining steps that it plans to take to remove or replace full SSNs it includes on mailed documents.
> - The number of documents and approximate mailing volume that it has yet to address.
> - The expected date by which it will stop mailing documents that contain full SSNs to individuals.

By requiring state agencies to report on specific privacy practices, this bill should not only aid those agencies in preparing to comply with the prohibition in this bill, but will also arguably give the Legislature valuable information that is necessary for this body to appropriately regulate state agencies who may be putting the privacy of California residents at risk and needlessly increasing their exposure to identity theft. At the same time, reports to the Legislature are generally available to the public. Thus, the reporting requirement in this bill would create a public list of state agencies that continue to send full SSNs, which could inform individuals planning on committing identity theft about specific pieces of mail to intercept from claimants. Accordingly, as this bill moves through the legislative process, the author may wish to consider an alternative reporting requirement whereby information that may create security risks is not available to the general public.

Staff additionally notes that this bill, which was amended last April, requires state agencies to report to the Legislature by September 1, 2020. Because the bill, if approved by the Legislature and signed by the Governor, will not go into effect until January 1, 2021, a technical amendment is needed to ensure state agencies are capable of compliance. The following amendment would change the date the reports are due to the Legislature to September 1, 2021.

Author's amendment:

On Page 3, line 11, strike "2020" and insert "2021"

Further, due to timing contraints, should this Committee approve the bill, this amendment will need to be processed by the Assembly Appropriations Committee.

6) **Requires that identity theft prevention and mitigation services be offered to individuals whose SSN has been improperly disclosed**: This bill would require any state agency that continues to send outgoing mail with full SSNs after January 1, 2023, to offer to provide at least one year of appropriate identity theft prevention and mitigation services to any individual whose full SSN was impermissibly mailed, along with all information necessary to take advantage of the offer.

   A similar requirement can be found within California's data breach notification law. Specifically, businesses or persons who own or license computerized data that includes personal information are required to disclose data breaches to the persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Additionally, if the person or business providing the notification was the source of the breach, they must also offer to provide identity theft prevention and mitigation services to the affected person, as specified. (*See* Civ. Code Sec. 1798.82.) Staff notes that this requirement under existing law is imposed only on private actors, not state agencies. That said, this Committee has approved efforts in the past that would have required government entities to extend identity theft and mitigation services to individuals affected by government data breaches. (*See* AB 241 (Dababneh, 2017).)

7) **Prior legislation**: SB 447 (DeSaulnier, 2012) would have prohibited a state agency from sending any communication to any individual that contains the full SSN of that individual unless required by federal law. SB 447 was vetoed by Governor Brown, who argued that this prohibition "would hinder the ability of state agencies to promptly and accurately provide information to run essential programs."

   SB 458 (Peace, Ch. Stats. 1998) *See* Comment 3.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200

Date of Hearing: January 14, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 699 (Grayson) – As Amended January 6, 2020

SUBJECT: Credit services organizations

SUMMARY: This bill would amend and update the Credit Services Act of 1984 (Act) by, among other things, requiring credit services organizations (CSOs) to provide consumers with monthly itemized statements, redact specified information in certain written communications, and creates statutory penalties for willful and knowing violations of the Act. Specifically, **this bill would**:

1) Require a CSO to provide a monthly statement to the consumer showing each service performed, including each call, letter, or other communication, and credit check made or sent on behalf of the consumer, and the date of each such service before charging the consumer any fees for the services.

2) Prohibit a CSO from engaging in the following activities:

   - Counseling a consumer to make an untrue statement to a data furnisher.
   - Seeking to remove adverse information from the consumer's credit record that is known, or that by the exercise of reasonable care should be known, to be accurate and not obsolete.
   - Calling or submitting any communication to a consumer credit reporting agency, creditor, debt collector, or debt buyer without the consumer's knowledge and consent.
   - Calling or submitting any communication to a consumer reporting agency, creditor, debt collector, or debt buyer impersonating a consumer and failing to identify when the communication originates from the CSO.
   - Submitting a consumer's dispute to a consumer credit reporting agency, creditor, debt collector, or debt buyer more than 180 days after the account subject to the dispute has been removed.
   - Sending any communication, directly or indirectly, to any person on behalf of a consumer without disclosing the sender's identity, street address, telephone number, and facsimile number, and, if applicable, the name and street address of any parent organization of sender.
   - Sending any communication on behalf of a consumer to any person other than the consumer without providing an exact copy of the communication to the consumer within five days thereafter.
   - Sending, or causing to be sent, any communication on behalf of a consumer that includes a notary acknowledgment without complying with the applicable laws regarding notary acknowledgments.

3) Requires a CSO to redact specified portions of personal information, such as a social security number and birth date, in written communications.

4) Extends the records retention requirement in current law from two years to four years.

5) Requires a contract between a CSO and consumer to include specified information, including a list of the adverse information appearing on the consumer's credit report, a list of those accounts that the CSO will seek to delete or modify and, if applicable, a definition of each modification sought and the anticipated payment required by the consumer to achieve each account deletion or modification.

6) Creates a civil penalty by which a consumer can recover between $100 and $1,000 for willful and knowing violations of the Act by a CSO.

7) Requires the AG to maintain on a publicly available internet website a list of registered CSOs along with any complaints submitted by consumers regarding each CSO, and requires consumers to be provided with a notice informing them that they can submit complaints about the services provided or the fees charged by a CSO to the AG, as specified.

8) Replace the term "buyer" with the term "consumer" throughout the Act.

9) Define "communication" to mean the conveyance of any information regarding a debt, credit record, credit history, or credit rating, directly or indirectly, to any person by any means or through any medium.

10) Define "consumer" to mean a natural person who is solicited to purchase or who purchases the services of a credit services organization.

11) Define "personal information" to mean a consumer's social security number, taxpayer identification number, state identification card number, financial account number, credit card number, debit card number, or date of birth. Notwithstanding the foregoing, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

12) Make other various changes to the Act.

EXISTING LAW:

1) Establishes the Credit Services Act of 1984 (Act), which generally defines and regulates the activities of credit services organizations (CSOs) (Civ. Code Sec. 1789.10 et seq.)

2) Defines a CSO as a person who, with respect to the extension of credit by others, sells, provides, or performs, or represents that he or she can or will sell, provide or perform, any of the following services, in return for the payment of money or other valuable considerations: (1) improving a buyer's credit record, history, or rating; (2) obtaining a loan or other extension of credit for a buyer; or providing advice or assistance to a buyer with regard to either (1) or (2). (Civ. Code Sec. 1789.12.)

3) Prohibits CSOs from engaging in certain specified activities including, among others:

- Charging or receiving any money or other valuable consideration prior to full and complete performance of the services the CSO has agreed to perform for or on behalf of the buyer.

- Making, or counseling or advising a buyer to make a statement that is untrue or misleading and that is known to be untrue or misleading to a consumer credit reporting agency or to a person who has extended credit to a buyer or to whom a buyer is applying for an extension of credit, as specified.

- Removing, or assisting or advising the buyer to remove adverse information from the buyer's credit record that is accurate and not obsolete.

- Making or using untrue or misleading representations in the offer or sale of the services of a CSO, including guaranteeing or otherwise stating that the CSO is able to delete an adverse credit history unless the representation clearly discloses that this can be done only if the credit history is inaccurate or obsolete and is not claimed to be accurate by the creditor who submitted the information.

- Engaging, directly or indirectly, in an act, practice, or course of business that operates or would operate as a fraud or deception upon a person in connection with the offer or sale of the services of a CSO.

- Advertising or causing to be advertised, in any manner, the services of the CSO, without being registered with the AG.

- Submitting a buyer's dispute to a consumer credit reporting agency without the buyer's knowledge. (Civ. Code Sec. 1789.13.)

4) Prohibits a CSO from providing a service to a buyer except pursuant to a written contract that must include a statement declaring the buyer's right to cancel the contract, the terms, and conditions of payment, a full and detailed description of the services to be performed by the CSO, and the estimated date by which the services are to be performed. (Civ. Code Sec. Section 1789.16.)

5) Requires, among other things, that a CSO register with the AG before conducting business in this State. The CSO applicant must, among other things, file a surety bond, pay a $100 registration fee, and annually file a renewal registration application with the AG. (Civ. Code Sec. 1789.25.)

6) Provides a private right of action for recovery of damages, or for injunctive relief, or both, related to a violation of the Act. Entitles a prevailing plaintiff to reasonable attorney's fees and costs, and authorizes a trial court to assess punitive damages. (Civ. Code Sec. 1789.21.)

7) Defines "buyer" as a natural person who is solicited to purchase or who purchases the services of a CSO. (Civ. Code Sec. 1789.12(c).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to increase transparency in the provision of credit repair services and increase enforcement of the Credit Services Act. This bill is sponsored by the California Association of Collectors.

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

> In recent years the activities of CSOs have come under scrutiny by the Federal Government and consumer watchdogs because of misleading practices and unlawful fees. While California has some of the strongest consumer protections in the nation for other industries, current law does not require CSOs to provide even basic information about the services they will render, or have rendered, how much their services are likely to cost, when they communicate with third parties on behalf of the consumer, or a timeline for when their services will be complete.
>
> AB 699 will enhance consumer protections and bring the Credit Services Act of 1984 into the 21st century by instituting the following requirements on CSOs:
>
> - Require that CSOs tell consumers what they intend to do and the results to be expected. This includes information on the credit items to be disputed or modified, the expected cost and the estimated date to be completed.
> - Require itemized receipts and disclosures to the consumer of the actions the CSO has taken before the CSO charges the consumer any fees.
> - Disclose to consumers and provide copies of all communication sent by a CSO on behalf of a client.
> - When sending a communication on behalf of a consumer to a 3rd party, require CSOs to disclose that the communication originated from a CSO and provide contact information for the sender.
> - Before entering into a contract with a consumer, require that a CSO provide a written statement stating that complaints with the service can be brought to the California Department of Justice and that a consumer credit report copy can be obtained free of charge.
> - Allow consumers to seek damages between $100 and $1000 for non-compliant CSOs.

3) **Business practices of credit repair organizations**: Subject to the Credit Services Act of 1984 (Act), credit repair companies are organizations that offer to improve a consumer's credit profile in exchange for a fee. Companies covered by the Act are required to register with the California Attorney General (AG) prior to engaging with California consumers and renew their registration annually.

Credit repair companies have been widely criticized for engaging in unfair and deceptive marketing and business practices and for charging high fees for services that consumers can often perform themselves. The Consumer Financial Protection Bureau (CFPB) has also taken

enforcement actions against credit repair companies for violations of federal law, including against four California-based companies. The CFPB actions are not limited to fines, but also include shutting companies down and banning them from providing any credit repair services. In May 2019, the CFPB filed suit against Lexington Law and CreditRepair.com. In the complaint, the CFPB alleges that Lexington Law relied on an expansive network of online lead generators that "used deceptive, bait advertising to generate referrals to Lexington Law's credit repair service." Late last year, Google announced that ads for credit repair services would no longer be allowed to serve on its advertising platform. In the updated policy, Google states that the company wants "consumers to make informed decisions about the services offered to help them address bad credit," and to protect users from harmful practices, an outright ban on credit repair advertisements is appropriate.

However, credit repair companies are not the only financial products and services receiving consumer complaints. In fact, when examining the nearly 1.5 million consumer complaints received as of April 1, 2018, the CFPB reported that over 400,000 were the result of debt collection activity, 314,068 were associated with credit reporting, 20,152 were associated with payday loans, and 1,633 were associated with credit repair. (*See* <https://files.consumerfinance.gov/f/documents/bcfp_complaint-snapshot_debt-collection_052018.pdf.> [as of Jan. 10, 2020]).

This bill is sponsored by the California Association of Collectors (CAC), representing the largest state organization of debt collectors. CAC argues that this bill is needed because member companies receive "robo letters, sent purportedly from the consumer and without disclosing the identity of the real sender." Under federal law, upon receiving disputes from consumers, debt collectors are required to conduct a reasonable investigation, report results to the consumer within 30 days, and provide specified notices to consumer reporting agencies. Central to CAC's position is the contention that if letters sent on *behalf* of the consumer do not identify that the correspondence is coming from a credit repair company, debt collectors incur costs that negatively affect the debt collector's profitability. Accordingly, among other things, this bill seeks to enact several provisions aimed at reducing the resources debt collectors must dedicate to addressing "robo letters" and other business practices of credit repair companies.

The California Bankers Association writes in support of this bill that "[u]nfortunately, creditors are often forced to research frivolous and false disputes made by credit repair services organizations. Deceptive practices employed by some organizations that promise to scrub negative credit files and improve credit scores for an upfront fee are in violation of multiple consumer protection statutes, including the Telemarketing Sales Rules and the Consumer Financial Protection Act. [...] [The] enhanced disclosure and transparency requirements [in this bill] are necessary for consumer protection and will help ensure that consumers have a better chance at an accurate credit report."

4) **Provisions in the bill that should benefit consumers, including statutory damages which should further increase enforcement of the Credit Services Act**: Existing law authorizes individuals who have been injured by a violation of the Act or by a credit services organization's breach of a contract to bring an action for recovery of actual damages, injunctive relief, or both, and reasonable attorney's fees and costs. In addition, the court may award punitive damages. (Civ. Code Sec. 1789.25.) This bill would additionally entitle a

consumer to a civil penalty between $100 and $1000 for knowing and willful violations of the Act.

By way of background, both state and federal law provide a number of protections to consumers who seek the services of CSOs. Despite these laws, some credit repair companies still operate in ways that exploit vulnerable individuals and/or violate the law.

Arguably, enforcement of existing law continues to be a challenge and keeps the various laws from achieving their full consumer-protection potential. Part of the challenge is that although a variety of actors are authorized to take different actions against CSOs for violations of the law, there is no licensing entity to whom CSOs are held accountable. On this point, recent correspondence from the AG notes:

> [U]nlike a traditional licensing program, such as those administered by the Department of Consumer Affairs or the Department of Business Oversight, [the credit services organization] registration program does not provide the Attorney General with authority to impose administrative fines or other sanctions against registrants. In the absence of this authority the program's staff takes informal actions, which may include sending non-registered credit services organizations a letter informing them of their obligations under the law in an effort to bring them into compliance, and requesting that applicants or registrants resolve consumer complaints identified as part of the application review process. This frequently results in the registrant or applicant providing refunds to the affected consumer. The Department also works with sister agencies, including city and district attorneys which have authority to enforce the Act (See Civil Code Section 1798.20), and with federal regulators, to provide support for enforcement actions undertaken by those agencies against registrants. The Act also includes a private right of action, allowing consumers who are harmed by a registrant to bring suit and, if successful, recover against the bond or deposit filed by the registrant with the Secretary of State.

Staff further notes that under existing law, the damages available to individuals who bring a private right of action are limited to actual damages, but in no case less than the amount paid by the consumer to the CSO. In practice, this means that most individuals who have a claim against a credit repair company may only recover what they paid the credit repair company, despite the amount of time spent or frustration experienced. By increasing the amount of damages one may recover for knowing and willful violations of the Act, this bill will arguably help incentivize private suits against bad actors in the credit repair service industry, thereby increasing enforcement.

Other provisions of the bill that will arguably benefit consumers include:

- Increasing the minimum time a CSO must maintain specified records from two to four years to align with the statute of limitations for breach of contract actions.

- Updating required notices to include specific information about the consumer and how the CSO will attempt to resolve adverse information on the consumer's credit report.

While these provisions should benefit consumers, as a matter of public policy it is equally important that consumers have access to law-abiding and ethical professionals to assist them with their financial needs. Thus it is crucial that requirements imposed on CSOs in the Act

are closely tied to protecting consumers and do not simply create operational burdens with no real consumer benefit so that enforcement of the Act through litigation does not limit the number of ethical professionals available to assist individuals.

5) **Various provisions of the bill arguably undermine consumer protections or benefits offered to consumers by CSOs**: This bill would include several provisions aimed at increasing transparency in CSO contracts and services. USCB, America, Inc., an employee-owned accounts receivable management company, writes in support that "AB 699 will ensure that the Credit Services Act of 1984 is updated to address new communications technologies that have emerged in the more than three decades since that law's enactment. Significantly, the bill will ensure that consumers are not deceived into having 'credit service organizations' dispute items on their credit reports that have already been removed or resolved. The bill will also prevent a credit service organization from impersonating a consumer, which will help ensure that all communications by these organizations are done on behalf of, and after consultation with, the consumer."

   While seemingly well-intended, some of these provisions may result in harm to consumers. For example, the bill would prohibit "impersonation" of a consumer by a CSO by requiring a CSO to identify when a communication originates from the CSO. In fact, the opposition to this bill argues that these provisions are intended to prevent consumers from receiving professional help when questioning what appears on their credit reports.

   Indeed, under the Federal Fair Credit and Reporting Act, data furnishers (which are debt collectors for the purposes of this analysis) have an obligation to investigate disputes about the information on credit reports from a *consumer* and to review all relevant information provided by the *consumer*. By contrast, there is no obligation imposed on a data furnisher to investigate disputes "prepared on behalf of the consumer by, or submitted on a form supplied to the consumer by, a credit repair organization." (12 C.F.R. Sec. 1022.43.) To this point, Lexington writes "proposed Civil Code section 1789.13(n) protects debt collectors rather than consumers since the debt collectors acknowledged intention is to ignore all correspondence from a credit services organization. The effect is to make the process more complicated for consumers by forcing them to spend their own time and effort, rather than enlisting the help of a professional. Ultimately, fewer consumers will assert their rights and those who do will be outmatched when battling large organizations on their own." Staff notes that the same arguably holds true for proposed Civil Code Sec. 1789.13(v) in the bill.

   Building on a provision in existing law that prohibits a CSO from removing or advising a consumer to remove an item from their credit report that is accurate and not obsolete, this bill would also prohibit a CSO from seeking to remove or assisting or advising a buyer to remove adverse information from the consumer's credit record that "by the exercise of reasonable care should be known" to be accurate and not obsolete. Lexington Law argues that this modification will harm consumers:

   > The proposed amendment to Civil Code section 1789.16(a)(3) imposes a requirement of knowing the answers to questions before they are asked. Particularly in the debt collection world, consumers often do not recognize items appearing on their credit report. Those items may or may not appropriately appear on a credit report and it may require some amount of investigation to arrive at that conclusion. Forcing consumers to know upfront whether an item needs to be deleted or modified before engaging a credit services

organization deprives them of the opportunity to receive professional help in assessing the fairness, accuracy, or substantiation of their credit report.

Finally, this bill would require the AG to maintain on a publicly available internet website a list of the credit services organizations that are registered in this State, along with any complaints the AG has received about those CSOs. The bill does not, however, require the AG to investigate those complaints. Thus, even complaints that the AG found to be frivolous, false, or unwarranted would be listed next to those complaints with merit. While a list of registered CSOs may be helpful to consumers who are vetting credit repair companies, unfiltered complaints could be confusing for consumers seeking to separate scrupulous from unscrupulous companies.

6) **Some provisions of the bill seemingly do no benefit consumers but create practical hurdles for CSOs**: This bill would define personal information to mean "a consumer's social security number, taxpayer identification number, state identification card number, financial account number, credit card number, debit card number, or date of birth," so long as the information is lawfully made available to the general public from federal, state, or local government records. The bill would then require the personal information to be redacted to the last for digits, as specified, in any written communication made by a CSO.

While redacting information that may increase the risk of a consumer falling victim to identity theft is a good practice that should be adhered to whenever possible, there are circumstances when the use of a redacted identifier would not achieve the desired objective. For example, limiting a person's birthday to only the month and year, may not adequately identify an individual if there are multiple persons with the same name born during that month. Additionally, sometimes full identifiers are required, and prohibiting the use of them in those circumstances would put CSOs in the difficult position of choosing between being able to perform the services they promised or violate the law, thereby subjecting them to statutory damages (*see* Comment 4 above).

Similarly, the bill would require CSOs to comply with the applicable laws regarding notary acknowledgments when sending communications on behalf of a consumer that includes a notary acknowledgment. This provision appears to operate only to ensure that a CSO follows the law, which they are already required to do, and would arguably subject them to liability under multiple statutory schemes for one violation.

Additionally, multiple provisions in the bill require a CSO to disclose specified contact information, including a facsimile number. While seemingly innocuous, such a requirement will expose CSOs who do not have a facsimile number to statutory damages. Other highly specific requirements would similarly expose CSOs to liability despite the violations not being closely connected to potential harm to a consumer. For example, in addition to the requirement under existing law that the CSO must complete any contracted-for service before charging a consumer for it, the bill would additionally require a CSO to send each consumer an itemized monthly statement showing each service performed, including each call, letter, or other communication, and credit check made or sent on behalf of the consumer, and the date of each such service before charging the consumer any fees for the services. This level of information does not necessarily benefit the consumer above what existing law requires, and may, in fact, be overwhelming.

Similarly, the bill would require a CSO to send an "exact copy" of any communication made on behalf of a consumer to that consumer within five days. Because the bill defines "communication" broadly, recordings of phone calls would need to be provided to consumers, along with every letter, message, text, or other communication made on their behalf. This amount of information would likely be overwhelming for a consumer, who had already agreed to have certain services performed on their behalf and would arguably be an operational burden for CSOs. Further, sending a mere copy (instead of an exact copy) of any of these communications would expose a CSO to liability despite not having acted in a way that would harm the consumer.

7) **Narrowing the bill may benefit consumers**: As discussed in the comments above, this bill contains several provisions that should benefit consumers who interact and contract with CSOs. At the same time, it also includes provisions that could seriously undermine any legitimate service that a CSO could offer a consumer in search of professional assistance. Further, other provisions expose CSOs to liability for acts or omissions that are not closely tied to the value of the service the consumer is receiving. Thus, in its current form, it is difficult to ascertain whether the bill, on balance, benefits consumers at all. To be true to the intent of the Credit Services Act, which this bill seeks to amend, the bill's provisions should be limited to those that truly benefit consumers.

   Accordingly, if this Committee were to approve this bill, it may wish to require the removal of the provisions that undermine the benefits a consumer may receive from legitimate credit repair services. Additionally the Committee may wish to require the removal of provisions that do not enhance consumer protection while simultaneously increasing liability for CSOs, as such liability can have the unintended consequence of driving up the cost of legitimate services for the exact individuals the bill should be designed to benefit.

   The author has agreed to the following amendments which would narrow the bill in the manner described above and better ensure that liability of CSOs is related to consumer benefit and harm. The amendments would:

   1) Eliminate the narrow definition of "personal information."

   2) Narrow the requirement that a CSO provide a monthly itemized statement to better reflect the services they contract to provide.

   3) Clarify that the burden falls on the CSO to exercise reasonable care in investigating wither adverse information on a consumer's credit record is accurate and not obsolete.

   4) Clarify that only copies of written communications need to be sent to a consumer.

   5) Eliminate duplicative requirements with regard to applicable laws regarding notary ackowledgments.

   6) Allow the inclusion of full social security numbers and other identifiers in written communications by CSOs when required by law or legally permissible and required to achieve the desired objective.

   7) Require a CSO to disclose a facsimile number only if applicable.

8) Remove the requirement that the AG list any complaints against a CSO on the publicly available website.

Additionally, the author has committed to working on the issues raised in Comment 5, above, whereby, requiring a CSO to identify themselves in correspondence could have the unintended consequence of permitting a data furnisher (under federal law) to disregard any correspondence sent on behalf of a consumer by a CSO. Thus, as the bill moves through the legislative process, the author commits to incorporating a requirement in the bill that a data furnisher shall treat any communication from a credit services organization sent on behalf of a consumer, as a direct communication from the consumer themselves. Incorporating this concept will likely require significant amendments to paragraphs (n) and (v) in Section 3 of the bill as well, which prohibit a CSO from "impersonating" a consumer and require a CSO to identify themselves in any correspondence on behalf of a consumer.

Author's amendments:

1) On page 5, strike lines 25-31

2) On page 6, line 6 strike "letter, or other" and insert "written"

   On page 6, lines 7-8 strike "before charging the consumer any fees for the services"

3) On page 6, line 31 after "known" insert "to the credit services organization"

   On page 6, line 32 after "known" insert "to the credit services organization"

4) On page 9, line 18 after "any" insert "written"

   On page 9, line 19 strike "an exact" and insert "a"

5) On page 9, strike lines 22-28

6) On page 9, line 39 after "birth" insert "unless inclusion of the full number or date is otherwise required by law or legally permissible and required to achieve the desired objective."

7) On page 13, line 3 strike "facsimile number, and"

   On page 13, line 4 strike "of the credit services organization" and insert "and facsimile number if applicable, of the credit services organization,"

8) On page 17, lines 22-24 strike "The Attorney General shall list any complaints submitted pursuant to subdivision (e) of Section 1789.15 regarding each credit services organization."

9) **Double-referral**: This bill is double-referred to the Assembly Banking Committee, where it is scheduled to be heard on January 13, 2020.

REGISTERED SUPPORT / OPPOSITION:

Support

California Association of Collectors (sponsor)
California Bankers Association
California Financial Services Association
USCB, America, Inc.

Opposition

Lexington Law

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200

Date of Hearing: January 14, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 904 (Chau) – As Amended January 6, 2020

SUBJECT: Search warrants: tracking devices

SUMMARY: This bill would specify that a "tracking device" includes any software that permits the tracking of the movement of a person or object for purposes of existing law, which allows a search warrant to be issued when the information to be received from the use of a tracking device constitutes evidence that: (1) tends to show that either a felony, or certain misdemeanors, has been committed or is being committed; (2) tends to show that a particular person has committed or is committing a felony or certain misdemeanors; or, (3) will assist in locating an individual who has committed or is committing a felony or certain misdemeanors.

EXISTING LAW:

1) Provides, pursuant to the U.S. Constitution, that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." (U.S. Const., 4th Amend.)

2) Governs search warrants, including the grounds upon which a search warrant may be issued. (Pen. Code Sec. 1523 et seq.) Among other things, existing law authorizes a search warrant to be issued when the information to be received from the use of a tracking device constitutes evidence that tends to show that either a felony, or a misdemeanor under the Fish and Game Code or Public Resources Code, has been committed or is being committed; tends to show that a particular person has committed or is committing a felony or such misdemeanor violations; or will assist in locating an individual who has committed or is committing a felony or such misdemeanor violations. (Pen. Code Sec. 1524(a)(12).)

3) Provides that a tracking device search warrant issued pursuant to the above provision must identify the person or property to be tracked and must specify a reasonable length of time, not to exceed 30 days from the date the warrant is issued, that the device may be used. Authorizes courts to grant one or more extensions for good cause, as specified. The search warrant must command the officer to execute the warrant by installing a tracking device or serving a warrant on a third-party possessor of the tracking data, as specified, and requires the execution of the warrant to be completed no later than 10 days immediately after the date of issuance. As used in this section, "tracking device" means any electronic or mechanical device that permits the tracking of the movement of a person or object. (Pen. Code Sec. 1534(b).)

4) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or electronic device information from any person or entity other than the authorized possessor of the device, absent a search

warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. CalECPA also generally specifies the only conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, consent of the owner of the device, or emergency situations, as specified. (Pen. Code Sec. 1546 et seq.)

5) Defines various terms for purposes of CalECPA, including the following:

- "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

- "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. "Electronic communication information" does not include subscriber information, as defined.

- "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

- "Electronic device" means a device that stores, generates, or transmits information in electronic form. An electronic device does not include the magnetic strip on a driver's license or an identification card issued by this state or a driver's license or equivalent identification card issued by another state.

- "Electronic device information" means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.

- "Electronic information" means electronic communication information or electronic device information. (Pen. Code Sec. 1546(c)-(h).)

FISCAL EFFECT: None. This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of this bill**: In addition to the existing prohibition on the use of tracking devices unless certain conditions are met, this bill seeks to ensure that government entities cannot use tracking *software* that permits the tracking of the movement of a person or object unless certain conditions are met. This bill is author-sponsored.

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

> The rights of individuals against unlawful search and seizure are enshrined in both the Constitutions of the United States (through the Fourth Amendment) and the State of California. Having stood for over 200 years, this basic human right has consistently been reinterpreted to account for changes in government, technology, and society. Judicial understanding of this right has morphed from an explicit right of privacy within the home and personal documents, to an expansive protection against the collection of information by the government in a great many applications. Most recently, the United States Supreme Court recognized in *Carpenter v. United States* that the use of cell phone location information by law enforcement is an invasion of personal privacy, which requires the granting of a search warrant.
>
> This decision certainly represents a landmark case in the jurisprudence of the Supreme Court, but had limited applicability to the residents of California because this specific requirement has been applied to law enforcement agencies in California since 2012. With the rest of the country following suit, it is important that California continues to look ahead at the changing landscape of technology and maintains the lead in protecting our residents against unlawful search and seizure.
>
> Penal Code Section 1534 currently requires search warrants prior to an officer "installing a tracking device or serving a warrant on a third-party possessor of the tracking data." It is, however, no longer necessary for an officer to make physical contact with a device, person, or vehicle to "install" a "device" in order to track an individual. On the contrary, a government official need only have wireless access to download tracking software that will provide investigators with far more information than just a person's or a vehicle's location. AB 904 closes this loophole by specifically prohibiting software-based tracking of individuals by law enforcement without a warrant. (Footnote citations omitted.)

3) **The Fourth Amendment and innovations in surveillance tools**: The Fourth Amendment states, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Const. 4th Amend.) Stated another way, it prohibits Government from intruding on a person's right of privacy in their person, home, papers, and effects, unless the Government first obtains a warrant issued upon probable cause supported by sworn testimony and stating the place to be searched and the persons or things to be taken possession of. A warrant, thus, demonstrates that the search and seizure is "reasonable" as required by the Fourth Amendment's prohibition against "unreasonable searches and seizures."

While much of the early Fourth Amendment search doctrine focused on whether the Government "obtains information by physically intruding on a constitutionally protected area," more recent judicial precedent recognizes that "property rights are not the sole measure of Fourth Amendment protections." (*See Carpenter v. United States* (2018) 138 S.Ct. 2206, 2213, citing (*U.S. v. Jones* (2012) 565 U.S. 400 and *Soldal v. Cook County* (1992) 506 U.S. 56.) In the seminal case of *Katz v. United States* 389 U.S. 347, 351, the U.S.

Supreme Court established that "the Fourth Amendment protects people, not places." In doing so, the Court "expanded our conception of the Amendment to protect certain expectations of privacy as well. When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the Supreme Court] has held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." (*Carpenter,* 128 S.Ct. at 2213.)

As described most recently by the Supreme Court in the case of *Carpenter* (discussed further in Comment 4, below) Fourth Amendment jurisprudence reflects certain basic guideposts in the Court's analysis of what is an unreasonable search and seizure, as informed by a historical understanding of that concept when the Fourth Amendment was first adopted. First, the amendment seeks "to secure 'the privacies of life' against 'arbitrary power.'" Second, and related, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" (*Id.* at 2214, internal citations omitted.) These guideposts apply when applying the Fourth Amendment to innovations in surveillance tools. "As technology has enhanced the Government's capacity to encroach on areas normally guarded from inquisitive eyes, [the] Court has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (*Id.*, internal citations omitted.)

By way of examples, the Court has applied the Fourth Amendment as follows to various emerging technologies:

- In *Smith v. Maryland* (1979) 442 U.S. 735, the court ruled that the Government's use of a pen register (a device that records the outgoing phone numbers dialed on a landline phone) was not a search. Noting the pen register's limited capabilities, the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." As such, when Smith placed a call, he was said to have "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." (*Id.* at 742, 744).

- In *United States v. Knotts* (1983) 460 U.S. 276, 281, 282, the Court considered the Government's use of a "beeper" to aid in tracking a vehicle through traffic as officers (with intermittent aerial assistance) followed the vehicle relying on the beeper's signal to keep the vehicle in view. There, the Court concluded that the "augment[ed]" visual surveillance did not constitute a search because a "person traveling in an automobile of public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."

- In *Kyllo v. United States* (2001) 533 U.S. 27, the Court determined that the Government could not capitalize on new sense-enhancing technology (thermal imaging) to explore what was happening within the home, absent a warrant.

- In *United States v. Jones* (2012) 565 U.S. 400, the Court was faced with a case wherein FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for almost 30 days. Based on the Government's

physical trespass of the vehicle, five justices agreed that related privacy concerns would be raised by, for example, "surreptitiously activating a stolen vehicle detection system" in Jones's car to track him, or conducting GPS tracking of his cell phone. Since GPS monitoring of a vehicle tracks every movement that a person makes in the vehicle, the concurring Justices in *Jones* concluded that "'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large." (*Carpenter*, 138 S.Ct. at 2215, internal citations omitted.)

- In *Riley v. California* (2014) 573 U.S. 373, the Court recognized the immense storage capacity of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone.

Like the holdings in many of these cases, this bill recognizes that laws require periodic updating to ensure that rights are protected in as new technologies become available. The California Attorneys for Criminal Justice (CACJ), a statewide association of criminal defense attorneys in private practice and working in public defender offices, writes in support of this bill:

> AB 904 would clarify that the prohibition on accessing an electronic device without a search warrant includes any software that permits the tracking of a person or object. This bill closes a loophole in the law that could allow for the software-based tracking of individuals by law enforcement without a warrant. Search warrants protect the public from unreasonable searches and seizures, a constitutional right that CACJ supports and believes should be expanded in the face of new technology.

4) ***Carpenter v. United States***: Most recently, in 2017, the U.S. Supreme Court was faced with a question of how the Fourth Amendment applies "to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals" in the case of *Carpenter v. United States* (2018) 138 S. Ct. 2206. Using the guidelines of the cases described in Comment 3, above, the Court analogized that the "tracking partakes of many of the qualities of the GPS monitoring [the Court] considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." (*Id.* at 2216.)

   In *Carpenter*, the Court examined the issue under two lines of Fourth Amendment cases. First, it outlined a line of Fourth Amendment cases (including *Knotts* and *Jones*, discussed in Comment 3, above) that addressed a person's expectation of privacy in his or her physical location and movements. Second, it reviewed another line of decisions (including *Miller* and *Smith*) wherein the Court has drawn a line between what a person keeps to himself and what he shares with others, which has come to be known as the third party doctrine[1]. The

---

[1] A doctrine stating that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (*Smith v. Maryland* (1979) 442 U.S. 735, 743-744), "even if the information is revealed on the assumption that it will only be used for a limited purpose." (*United States v. Miller* (1976) 425 U.S. 435, 443). In those cases, the Government is typically free to obtain such information from the recipient without triggering the Fourth Amendment requirement for a warrant.

Carpenter Court ultimately held that the government's acquisition of Carpenter's cell-site records was a search for purposes of the Fourth Amendment and required a warrant.

5) **The California Electronic Communications Protection Act**: As noted by the author above, while instructive on how the Supreme Court may apply existing protections to emerging technologies in the near future, *Carpenter* had limited applicability in this state, as California has protected this information for a number of years. California also provides extensive protection to Californians by way of the California Electronic Communications Protection Act (CalECPA), but there does appear to be some question of whether the protection is comprehensive.

Enacted in 2015 by SB 178 (Leno, Ch. 651, Stats. 2015), CalECPA generally prohibits government entities from either: (1) compelling the production of or access to "electronic communication information" from a service provider; or, (2) compelling the production of or access to "electronic device information" from any person or entity other than the authorized possessor of the device. CalECPA authorizes such actions only in limited circumstances. Chief among these authorized circumstances is where the government entity properly obtains a warrant pursuant to existing state law generally governing the issuance of warrants and additional CalECPA warrant requirements. (*See* Pen. Code Sec. 1946.1(a)(1)-(2), (b) and (d).)

Further, CalECPA specifically prohibits government entities from accessing *electronic device information* by any means of physical interaction or *electronic communication* with the *electronic device*, outside of limited circumstances, which include where a warrant has been obtained consistent with those same laws. "Electronic device information" means any information stored on or generated through the operation of an *electronic device*. "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system. "Electronic device" includes any information stored on or generated through the operation of an electronic device.

Notably, this provision does not appear to limit the ability of government entities from accessing "electronic communication information" by means of physical interaction or electronic communication with the electronic device. "Electronic communication information" generally means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or *location of the sender or recipients at any point during the communication*, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address.

Stated another way, because CalECPA only: (1) limits the ability of a government entity from obtaining "electronic communication information" from a service provider; (2) limits the ability of a government entity to obtain "electronic device information" from any person or entity other than the authorized possessor of the device; and (3) only limits the ability of a government entity to access "electronic device information" by means of physical interaction or electronic communication with the electronic device, it appears possible for law

enforcement to obtain "electronic communication information" by means of physical interaction or electronic communication with an electronic device.

Additionally, CalECPA appears entirely silent on the issue of the ability of government to compel access to or surreptitiously access by physical interaction with *software* on a device. Because of this ambiguity, AB 904 seeks to ensure that the law is absolutely clear, by prohibiting the tracking of individuals through software without a warrant.

Two civil liberties groups, the American Civil Liberties Union of California (ACLU) and the Electronic Frontier Foundation, interpret the bill differently and are concerned that the bill would instead *authorize* software-based tracking by law enforcement. Writing in opposition, the ACLU argues:

> Allowing law enforcement use of tracking software that can be installed on a person's telephone or other electronic equipment without the person's knowledge poses a host of dangers to the privacy rights of Californians. Such software might also allow law enforcement access to more than just location information. For example, if spyware were installed on an individual's phone, that software could not only allow law enforcement to tack that person's location but also to access the phone's camera, listen in on conversations, see the person's activity on the phone, and collect other sensitive information.
>
> While we appreciate [the author's] intent to ensure that any law enforcement use of tracking software be carefully restricted under the law, in its current form, AB 904 unfortunately appears instead to authorize the use of software for tracking purposes when it is unclear whether law enforcement has the authority to install such software for that purpose under existing law. At a minimum, we believe that the bill should be amended to clarify that it does not authorize law enforcement installation or use of any software that was not previously authorized under law.

In response to these concerns, the author offers the following amendment which would clarify that the bill does not authorize the use of tracking software, but instead safeguards against it.

> Author's amendment:
>
> On Page 3, after line 18 insert *"(7) As used in this section, the reference to "software" is not intended to expand the authority of a government entity to use software for surveillance purposes under this chapter or any other law."* and renumber accordingly.

This amendment is consistent with the intent of the bill which seeks to strengthen and update California law by ensuring that: (1) government entities cannot obtain "electronic communication information" by way of physical interaction or electronic communication with an electronic device; and (2) government entities cannot obtain access to software on an individual's electronic device by either physical interaction or compelling a third party to provide that access, surreptitiously, unless the government entity follows California law governing wiretaps.

6) **Prior legislation**: AB 1924 (Low, Ch. 511, Stats. 2016) provided an exemption from CalECPA for pen registers and trap and trace devices to permit authorization for the devices to be used for 60 days.

SB 178 (Leno, Ch. 651, Stats. 2015) enacted CalECPA, which generally requires law enforcement entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.

AB 929 (Chau, Ch. 204, Stats. 2015) authorized state and local law enforcement to use pen register and trap and trace devices under state law, and permitted the issuance of emergency pen registers and trap and trace devices. The authorization for the use of a trap and trace device or a pen register was for 60 days from the date of issuance, with extensions of up to 60 days. However, the governor signed AB 929 prior to signing the ECPA and as a result, the authorization was chaptered out by the ECPA's 10-day authorizations.

SB 467 (Leno, 2013) would have required a search warrant when a governmental agency is seeking the contents of a wire or electronic communication that is stored, held, or maintained by a provider. SB 467 was vetoed by Governor Brown, who wrote: "The bill, however, imposes new notice requirements that go beyond those required by federal law and could impede ongoing criminal investigations. I do not think that is wise."

SB 1434 (Leno, 2012) would have required a government entity to get a search warrant to obtain the location information of an electronic device. SB 1434 was vetoed by Governor Brown, who wrote: "It may be that legislative action is needed to keep the law current in our rapidly evolving electronic age. But I am not convinced that this bill strikes the right balance between the operational needs of law enforcement and individual expectations of privacy."

SB 914 (Leno, 2011) would have required a search warrant to search the contents of a portable electronic device that is found during a search incident to an arrest. SB 914 was vetoed by Governor Brown, who wrote: "This measure would overturn a California Supreme Court decision that held that police officers can lawfully search the cell phones of people who they arrest. The courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections."

REGISTERED SUPPORT / OPPOSITION:

Support

California Attorneys for Criminal Justice

Opposition

American Civil Liberties Union of California
Electronic Frontier Foundation

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200

Date of Hearing: January 14, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 325 (Ramos) – As Amended January 6, 2020

SUBJECT: Self-service storage facilities

SUMMARY: This bill would remove the sunset date authorizing self-storage facility owners to email lien notices and related documents to self-storage unit occupants whose payments are overdue, and would provide these owners with an additional method of demonstrating actual delivery and receipt of such emails. Specifically, **this bill would**:

1) Permit the owner of a self-storage facility to demonstrate actual delivery and receipt of preliminary lien notices, notices of lien sales, and blank declarations in opposition to lien sales sent by electronic mail to the occupant of a self-storage unit if the occupant replies to the email communication, and there is evidence demonstrating the delivery path of the reply email.

2) Remove a January 1, 2021 sunset on certain statutory provisions authorizing self-storage facility owners to communicate with occupants via email.

3) Makes various other non-substantive technical changes.

EXISTING LAW:

1) Establishes the California Self-Storage Facility Act to regulate the relationship between owners of self-storage facilities and occupants of units within those facilities. (Bus. & Prof. Code Sec. 21700 et seq.)

2) Requires every contract for the rental or lease of storage space in a self-service storage facility to be in writing and to contain a statement that the occupant's property will be subject to a claim of lien and may even be sold to satisfy the lien if rent or other charges remain unpaid for 14 consecutive days. (Bus. & Prof. Code Sec. 21712(a).)

3) Permits, if the rent or other charges due for an individual storage space remain unpaid for 14 consecutive days, the owner of the self-storage facility to terminate the right of the occupant to use that storage space, by sending a preliminary lien notice to the occupant's last known address, and to a specified alternative address if the occupant has provided one. (Bus. & Prof. Code Secs. 21703 and 21712(b).)

4) Requires that a preliminary lien notice contain, among other things, an itemized statement of the owner's claim showing the sums due at the time of the notice and the date on which the sums became due, and a statement that the occupant may, not less than 14 days after mailing of the notice, be denied access to the storage space if all sums due are not paid by that date and that an owner's lien may be imposed thereafter. (Bus. & Prof. Code Secs. 21703 and 21712.)

5) Permits the owner, if the lien attaches, to deny the occupant access to the storage space, enter the space, and remove any property therein to a place of safekeeping. (Bus. & Prof. Code Secs. 21705 and 21712(b).)

6) Requires the owner, if it takes any of the actions set forth immediately above, to send to the occupant's last known address and to a specified alternative address, if the occupant has provided one, a notice of lien sale and a blank declaration in opposition to lien sale. (Bus. & Prof. Code Sec. 21705(b).)

7) Permits the owner to send the preliminary lien notice, the notice of lien sale, and the blank declaration in opposition to lien sale by any of these methods:

   - certified mail, postage prepaid;
   - regular first-class mail, if the owner obtains a certificate of mailing indicating the date the notice was mailed; or
   - electronic mail, subject to the conditions outlined below. (Bus. & Prof. Code Secs. 21703 and 21705(b).)

8) Places the following conditions on the use of electronic mail to send the preliminary lien notice, the notice of lien sale, and the blank declaration in opposition to lien sale:

   - The rental agreement must state that lien notices may be sent to the occupant and the alternative address by electronic mail.
   - The occupant must provide a written signature on the rental agreement consenting to receive lien notices by electronic mail.
   - The occupant must provide an email address as their last known address in either the latest rental agreement or in a subsequent written notice of change of address. (Bus. & Prof. Code Sec. 21712.)

9) Provides that an owner may demonstrate actual delivery and receipt of notices sent by electronic mail by any of the following methods:

   - the occupant acknowledges receipt of the electronic transmission of the record by executing an electronic signature, defined as an electronic sound, symbol, or process attached to, or logically associated with, an electronic record and executed or adopted by a person with the intent to sign the electronic record;
   - the record is posted on the owner's secure internet website, and there is evidence demonstrating that the occupant logged onto the licensee's secure Internet Web site and downloaded, printed, or otherwise acknowledged receipt of the record; or
   - the record is transmitted to the occupant through an application on a personal electronic device that is secured by password, biometric identifier, or other technology, and there is evidence demonstrating that the occupant logged into the application and viewed or otherwise acknowledged receipt of the record. (Bus. & Prof. Code Sec. 21712(c).)

10) Provides that if the owner is unable to demonstrate actual delivery and receipt of the electronic email, the owner shall resend the notice by mail to the occupant's last known mailing address in the manner originally specified by for that particular notice. (Bus. & Prof. Code Sec. 21712 (c).)

11) Establishes sunset dates of January 1, 2021 for the notice by electronic mail provisions above.

FISCAL EFFECT: None. This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of the bill**: This bill seeks to lift various sunsets in the California Self-Service Storage Facility Act, thereby permanently allowing electronic delivery of certain legal notices to self-storage unit occupants whose payments are overdue and would also provide facility owners with a new method to demonstrate actual delivery and receipt of those emails. This bill is sponsored by the Self Storage Association.

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

> AB 1108 (Daly) (2017) … provided the direct precedent for AB 325. This bill modified rules that govern how self-storage facility owners may send important notices to customers ("occupants") who miss a deadline for paying rent for their storage space and face a potential lien sale of their stored property. These changes allowed self storage providers to notify customers of liens by email, which would be confirmed either by electronic signature by the recipient or through proof of delivery by the self storage owner. This bill also allowed owners to perform lien sales on internet auction websites, clarifying state law to meet owners' understanding of contemporary law.
>
> This bill is necessary to avoid the onslaught of red tape for local small businesses, which would follow if self storage businesses were forced to move backwards to mail-only service. This bill keeps an effective practice going, and allows self storage businesses across our state to continue operating with effective, streamlined practices.

3) **Self-service storage in California**: The California Self-Service Storage Facility Act took effect on January 1, 1981, and was updated in 2010 to allow owners to send lien notices by way of verified mail as opposed to only by certified mail. This modification made sending lien notices more efficient and less expensive than using certified mail. Because communication by email has become the preferred method of communication for many consumers, the Act was amended again in 2017 to allow for email notification. (*See* AB 1108 (Daly, Ch. 227, Stats. 2017).) Given the transitory circumstances of many self-storage customers, email is often a more effective means of contact than a mailing address but presents other challenges, as discussed more below.

   Under the Self-Service Storage Facility Act, after the occupant is 14 days overdue in paying storage fees for the unit, the facility owner may mail a preliminary lien notice to inform the occupant that if the overdue fees are not paid, a lien may attach to the stored property after 14 more days, and the occupant's right to use the storage space may be terminated.

On the 28th day that the storage fees remain unpaid, a lien attaches and the owner may mail to the occupant the notice of lien sale and a blank Declaration of Opposition to Lien Sale (declaration) to be completed and returned by the occupant. In addition, the occupant may be denied access to the storage space thereafter.

The notice of lien sale informs the occupant that the lien sale may, at earliest, occur after another 14 days (*i.e.,* on the 42nd day after the fees were due), and the declaration allows the occupant to state his opposition to the lien sale and informs him of his existing rights under law. If the occupant signs and returns the declaration to the owner before the date of the lien sale specified in the notice, then the owner must file suit against the occupant to enforce the lien. If the declaration is not returned in time, then the owner may proceed with the lien sale.

In 2017, this Committee approved AB 1108 (Daly, Ch. 227, Stats. 2017), which, among other things, established a framework for self-storage facility owners to provide the various legal notices discussed above to customers by email. While email has certain advantages over traditional mail (it is cheaper to send, and it may be better suited to reach homeless individuals), it is also relatively unreliable compared to U.S. mail. This unreliability is of particular concern because the Act gives occupants limited time to respond to notices to prevent lien sales of their stored property. Accordingly, AB 1108 provided the following safeguards as a condition of using email to deliver lien notices:

- The occupant must have opted-in to receive lien notices via email by providing a signed consent on the rental agreement.
- The owner must be able to establish actual delivery and receipt of emailed documents, as specified.
- If the owner cannot demonstrate actual delivery and receipt of an emailed document, then the owner must re-send the document by U.S. mail.

Consistent with other bills that similarly authorize the use of email for notification purposes, AB 1108 included a January 1, 2021, sunset date to the email notice provisions. By creating that three-year test period, the Committee argued that the Legislature would be given an opportunity to evaluate the utilization and effectiveness of electronic notice in the self-storage context before allowing it in perpetuity.

This bill would now remove those sunsets and allow for an additional method whereby self-storage facility owners may demonstrate actual delivery and receipt of email notices.

4) **Lifting the sunset and allowing reply emails to serve as evidence of actual delivery and receipt**: This bill has been in print for nearly a year and this Committee has received no feedback that emailed notices are harming self-storage unit occupants. Without any issues being brought to the attention of the Legislature, it appears to be an appropriate time to lift the sunset.

In addition to lifting the sunset on the three methods by which self-storage facilities can demonstrate actual delivery of email notifications, this bill would also create an additional method by which an owner can demonstrate actual delivery and receipt of an email notice. As introduced, this bill would have permitted self-storage unit owners to demonstrate actual delivery and receipt of relevant documents simply if the owner possessed an electronic

receipt of delivery to the occupant's last known address. This method was deemed insufficient, however, because it would not have required the occupant to take an affirmative, non-automated step in response to the delivery of the notice. Recent amendments now require a reply email from the occupant, along with evidence demonstrating the delivery path of the reply email. This amendment ensures that self-storage facility owners cannot forge reply emails, and also requires an affirmative step on the part of the occupant which is an indication that the occupant received the initial email containing the notice of lien.

To be consistent with prior Committee approvals of provisions dealing with email notification, a three-year sunset should be added to this newly added method of demonstrating actual delivery of email notice, so that the Legislature can ensure that consumers are sufficiently protected, and there are no unintended consequences.

Suggested amendments:

On Page 7, line 36 after "email." add "*This subparagraph shall remain in effect only until January 1, 2024, and as of that date is repealed.*"

5) **Prior legislation**: AB 1108 (Daly, Ch. 227, Stats. 2017) established a framework for self-storage facility owners to provide legal notices to customers by email.

AB 983 (Melendez, Ch. 778, Stats. 2014) would have required the occupant of a self-storage unit to bring a court action to stop a lien sale of his property, rather than requiring the owner of the facility to file suit to enforce the lien. Among other things, the bill also would have allowed lien-related notices to be emailed instead of being sent by mail. Those provisions were later amended out of the bill.

AB 655 (Emmerson, Ch. 439, Stats. 2010) revised the preliminary lien notice, declaration of objection, and made other related changes to the enforcement process for self-storage liens.

6) **Double-referral**: This bill is double-referred to the Assembly Judiciary Committee, where it is scheduled to be heard on January 14, 2020.

REGISTERED SUPPORT / OPPOSITION:

Support

California Self Storage Association (sponsor)

Opposition

None on file

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200

Date of Hearing: January 14, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1263 (Low) – As Amended January 6, 2020

SUBJECT: Contracts: consumer services: consumer complaints

SUMMARY: This bill would prohibit contracting for, or to propose to contract for, an agreement to not file a complaint with a licensing board or to participate in a license board's investigation into a licensee for a consumer service. Specifically, **this bill would**:

1) State that any waiver of the provisions of this section is contrary to public policy and is void and unenforceable.

2) Provide that violation of this section by a licensee shall constitute unprofessional conduct subject to discipline by the licensee's licensing board.

3) Define "consumer service" to mean any service which is obtained for use primarily for personal, family, or household purposes.

4) Define "licensing board" to mean any entity contained in Section 101 of the Business and Professions Code, the State Bar of California, the Department of Real Estate, or any other state agency that issues a license, certificate, or registration authorizing a person to engage in a business or profession.

EXISTING LAW:

1) Provides that certain contracts are unlawful if contrary to an express provision of law; contrary to the policy of an express law, though not expressly prohibited; or otherwise contrary to good morals. (Civ. Code Sec. 1667.)

2) Prohibits a contract or proposed contract for the sale or lease of consumer goods or services from including a provision waiving the consumer's right to make any statement regarding the seller or lessor or its employees or agents, or concerning the goods or services, and deems any waiver of that prohibition contrary to public policy and unenforceable. (Civ. Code Sec. 1670.8.)

3) Establishes the Department of Consumer Affairs (DCA) within the Business, Consumer Services, and Housing Agency. (Bus. & Prof. Code Sec. 100.)

4) Provides that the DCA is comprised of thirty-seven licensing boards, bureaus, committees, and commissions, each responsible for regulating various professionals. (Bus. & Prof. Code Sec. 101.)

5) Provides that all boards within the DCA are established for the purpose of ensuring that those private businesses and professions deemed to engage in activities which have potential impact upon the public health, safety, and welfare are adequately regulated in order to protect the people of California. (Bus. & Prof. Code Sec. 101.6.)

6) States that it is the duty of the Director of Consumer Affairs to receive complaints from consumers concerning violations of provisions of this code relating to businesses and professions licensed by any agency of the DCA. (Bus. & Prof. Code Sec. 325.)

7) Establishes the State Bar of California as the entity responsible for regulating legal professionals. (Bus. & Prof. Code Sec. 6000 et seq.)

8) Establishes the Department of Real Estate as the entity responsible for regulating real estate professionals. (Bus. & Prof. Code Sec. 10000 et seq.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to prohibit certain unconscionable provisions in consumer contracts. This bill is author-sponsored.

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

> Existing law has already been enacted with the intent to prohibit non-disparagement clauses in consumer contracts. This bill has been introduced [because] companies providing professional services are nevertheless seeking to restrict their customer's authority to make substantiated complaints to regulatory boards through refund agreements and other contracts. This bill would expressly prohibit these provisions in any contract governing the provision of professional services that are subject to licensure and oversight by the state.

3) **Background**: During the 2019 sunset review of the Dental Board of California by the Senate and Assembly Committees on Business and Professions Committee, it was uncovered that certain companies offering direct-to-consumer orthodontics products were providing dental services using a lesser standard of diagnostic review than traditional dental offices. Presumably, as a way of preventing consumers from making complaints about any adverse outcomes relating to this service model, one of the larger companies was requiring customers who sought a refund to sign an agreement that they would not disparage the company. The agreement was intended to be kept confidential and required the patient to promise not to "make public, disseminate, release or otherwise reference, allude to, suggest to any person, agency or other entity … the terms or existence of this General Release."

4) **Limitations on contracting for secrecy to further the public interest**: Secret settlements, non-disparagement, and non-disclosure clauses frequently raise public policy concerns with requiring an individual to waive their right to speak or report misconduct to authorities. Existing law disfavors the secret settlement of certain civil actions in which the public has a strong interest in the rights of the individual to disclose certain information about businesses and licensees.

   As a general matter, a contract should be interpreted in a manner that will make it lawful, operative, definite, reasonable, and capable of being carried into effect, if it can be done without violating the intention of the parties. At the same time, "a contract provision unlawful if it is contrary to an express provision of law; contrary to the policy of express law,

though not expressly prohibited; or, otherwise contrary to good morals." (Civ. Code Sec. 1667.)

Increasingly, the Legislature has scrutinized, and prohibited nondisclosure agreements when countervailing public policy supports individual rights to both settle legitimate claims and also make public if desired, the basis for the claims. In 2018, the Legislature passed SB 820 (Leyva, Ch. 953, Stats. 2018) to prohibit contracting for secrecy imposed on individuals who settle claims for specified sexual assault or harassment offenses. It also passed AB 3109 (Stone, Ch. 949, Stats. 2018) to prohibit contracting for a party to waive the right to testifying in an administrative, legislative, or judicial proceeding concerning alleged criminal conduct or alleged sexual harassment of a party to the contract. Similarly, in 2016, the Legislature prohibited gag clauses in settling a civil case of sexual abuse of a minor, or an elder or dependent adult. In the same vein, the State Bar has the authority to investigate an attorney who advises (or demands) that a party or client sign a confidential settlement agreement in a civil action in specified cases.

The Legislature's actions to explicitly bar certain contracting activity serves to ensure that unenforceable contracts are not entered into in the first place, thereby protecting consumers and providing redress for consumers if companies and their legal counsel include in their contracts provisions that are contrary to public policy. Additionally, declaring that certain contractual provisions are void and unenforceable ensures compliance and thwarts attempts to keep unlawful contracts secret due to confidentiality clauses. The effect is to promote integrity in contracting generally.

This bill seeks to accomplish a similar purpose by establishing that a licensee regulated by the State should not be permitted to suppress misconduct or other potentially embarrassing information by limiting an individual's ability to report the activity about a licensee's business practice to authorities. Too often, companies settling disputes bargain for secrecy as a matter of course. The bargaining power generally weighs in favor of the companies, who typically draft settlement agreements and ultimately can compensate the individual or require litigation. This bill shifts this power to permit the consumer to both settle valid claims and report misconduct to licensing authorities.

5) **Regulation of speech on matters of public concern**: Libel laws exist to protect companies from false and malicious speech. To the extent that a person makes statements of fact that are false and which harm the reputation of the identifiable licensee or company, the laws of defamation stand to provide redress for the defamed. (Civ. Code Secs. 44-46.) That being said, when the State regulates a person's professional activity through licensing boards, that person agrees to be subject to scrutiny to maintain their license. For this reason, suppressing any claim of misconduct or preventing a consumer from reporting to a licensing entity potential misconduct, is contrary to public policy and the purpose of licensing generally. Indeed, free speech principles support reporting unlawful activity. The right to speak freely in public forums on public matters is enshrined in California's constitution and laws, including the state's anti-SLAPP statute. (Code Civ. Proc. Sec. 425.16.)

A SLAPP suit is a "Strategic Lawsuits against Public Participation;" a lawsuit that seeks to use the court to squash speech that is of public concern. Under the anti-SLAPP statute, lawsuits that hinder a person's right of petition or free speech are subject to a special motion to strike which stays litigation and demands the prompt resolution of the SLAPP motion.

The findings and declarations of the anti-SLAPP statute provide that "it is in the public interest to encourage continued participation in matters of public significance." The anti-SLAPP statute seeks to ensure that this public participation "should not be chilled by abuse of the judicial process." It encompasses activities protected under the First Amendment and California's constitution, including petitioning the government for the redress of grievances.

Contract provisions that prevent individuals from reporting to government entities important information of misconduct are subject to scrutiny under anti-SLAPP laws. This bill, like the anti-SLAPP law, seeks to ensure that nondisclosure agreements will not chill public participation in matters of public significance.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200