SENATE JUDICIARY COMMITTEE
Senator Hannah-Beth Jackson, Chair
2019-2020 Regular Session

AB 1782 (Chau)
Version: August 11, 2020
Hearing Date: August 13, 2020
Fiscal: Yes
Urgency: No
CK

SUBJECT

Personal information: contact tracing

DIGEST

This bill regulates public entities and businesses engaging in technology-assisted contact tracing.[1]

EXECUTIVE SUMMARY

Contact tracing is a critical component in fighting the spread of infectious diseases. It has been traditionally conducted by public health officials to identify those infected, those who have come into contact with the infected individuals, and working with all parties to disrupt the spread of the disease. Given the worldwide COVID-19 pandemic, the importance of contact tracing has been brought to the fore. But the scale at which it must be conducted and the introduction of digital applications and platforms raises serious privacy concerns and calls for stronger protections of individuals.

This bill regulates public entities and businesses engaging in technology-assisted contact tracing (TACT). It provides clear guidelines on who can engage in TACT, what information can be collected, and how long it can be kept. It implements use and disclosure limitations. The bill requires the affirmative, informed consent of a user before any data can be collected or used and prohibits any discrimination based on participation in TACT.

This bill is author-sponsored. It is supported by AARP and the California Immigrant Policy Center. It is opposed by a coalition of industry and technology organizations, including the California Chamber of Commerce.

[1] This analysis is of the bill as amended on August 11, 2020. Such amendments were taken in response to Committee and stakeholder concerns.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

2) Establishes, pursuant to the federal Health Insurance Portability and Accountability Act (HIPAA), privacy protections for patients' protected health information and generally provides that a covered entity, as defined (health plan, health care provider, and health care clearing house), may not use or disclose protected health information except as specified or as authorized by the patient in writing. (45 C.F.R. § 164.500 et seq.)

3) Prohibits, under the State Confidentiality of Medical Information Act (CMIA), providers of health care, health care service plans, or contractors, as defined, from sharing medical information without the patient's written authorization, subject to certain exceptions. (Civ. Code § 56 et seq.)

4) Establishes the Information Practices Act of 1977 (IPA), which declares that the right to privacy is a personal and fundamental right and that all individuals have a right of privacy in information pertaining to them. It regulates the handling of personal information in the hands of *state* agencies. The IPA states the following legislative findings:

    a) the right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies;
    b) the increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information; and
    c) in order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798 et seq.)

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

6) Provides consumers the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces

of personal information the business has collected. A business must provide the information upon receipt of a verifiable consumer request. (Civ. Code § 1798.100(a), (c).)

7) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice, as specified. (Civ. Code § 1798.100(b).)

8) Provides consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)

9) Provides consumers the right to request that a business that collects personal information about the consumer, or that sells that information, to disclose to the consumer certain specified details. (Civ. Code § 1798.110(a), 1798.115(a).)

10) Provides a consumer the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. (Civ. Code § 1798.120.)

This bill:

1) Establishes the Technology-Assisted Contact Tracing Public Accountability and Consent Terms (TACT-PACT) Act, which generally regulates business and public entity engagement in TACT, which is defined as the use of a digital application or other electronic or digital platform that is capable of independently transmitting information and is offered to individuals for the purpose of identifying and monitoring individuals, through data collection and analysis, who may have had contact with an infectious person as a means of controlling the spread of a communicable disease. The use of devices at certain health facilities is exempted if only used within the facility's campus.

2) Places a series of obligations and restrictions on businesses and public health entities offering TACT and specifically prohibits other public entities from offering TACT. The bill requires these entities and businesses to secure a user's consent before they collect, use, maintain, or disclose a user's data and prohibits them from requiring any user, including an employee or contractor, to participate. Businesses and public health entities are also prohibited from discriminating against or penalizing a user based on participation in TACT. They are also required to do the following:

a) ensure that a request for an individual's consent details the public health purposes for the data, and the party or parties to whom that data will be disclosed;
b) provide a simple mechanism for a user to revoke consent at any time;
c) disclose to the user the categories of data collected, used, or disclosed and the specific public health purposes for which each category will be collected, used, or disclosed;
d) provide users with an effective mechanism by which to access, correct, and delete their personal information;
e) delete any personal information collected pursuant to TACT within 60 days from the time of collection. All other data must also be deleted within 60 days of collection except for specified research purposes;
f) ensure that all components of TACT are capable of being temporarily disabled and removed by the user in a manner that is clear, simple, and does not include any unnecessary steps;
g) encrypt any data collected and maintained pursuant to TACT to the extent practicable;
h) clearly and conspicuously disclose that the absence of an exposure notice does not ensure that the individual has not been exposed to the condition of public health concern;
i) issue a public report, at least once every 90 days, containing specified information;
j) implement and maintain reasonable security procedures and practices, appropriate to the nature of the data and the purposes for which that data will be used.

3) Restricts, except as provided, public health entities and businesses from associating data collected from a user pursuant to TACT in any way with data otherwise collected or maintained for other purposes. Personal information collected, used, or maintained by a public health entity through TACT shall not be used for any purpose other than facilitating the response to the immediate public health purpose.

4) Provides that it shall not be construed to limit or prohibit a public health entity or its agent from administering programs to identify individuals who have contracted, or may have been exposed to, a public health condition through traditional means intended to monitor and mitigate the transmission of a disease or disorder, including interviews, outreach, case investigation, and other recognized investigatory measures.

5) Requires that any data collected by, and any inventions, discoveries, intellectual property, technical communications, and records originated or prepared by, the contractor in the course of activities governed by the contract, including papers,

reports, charts, computer programs, and other documentation, be the public health entity's exclusive property.

6) Requires a public TACT contract to include certain provisions, including the following:

    a) participation in TACT, and any behavior or furnishing of information or consent for the purpose of effectuating TACT, shall be entirely voluntary;
    b) except as provided, the contractor shall comply with the requirements imposed on public health entities;
    c) performance metrics for evaluation of the particular goods or services provided pursuant to the contract;
    d) the term of the contract shall not exceed one year;
    e) limitations on data collection and use;
    f) security and data breach requirements;
    g) a contractor shall provide any source code created by the contractor pursuant to a TACT contract to the public health entity and any entity charged with oversight of the public health entity's acquisitions;
    h) a contract governed by this part shall be deemed a contract for the acquisition of information technology goods and services related to information technology projects for purposes of Section 12100.

7) Requires a public TACT contract to also prohibit a contractor from certain actions, including reidentifying or attempting to reidentify deidentified, anonymized, or aggregated data, or collecting data that is not directly necessary for the public health purposes enumerated in the contract.

8) Requires a business providing TACT that is not affiliated with a public health entity to clearly and conspicuously disclose upon solicitation and provision of a TACT service that the service is not affiliated with a public health entity. Such a business is restricted from all of the following:

    a) holding itself out to be affiliated with a public health entity;
    b) associating data collected from a user pursuant to TACT in any way with data otherwise collected or maintained for other purposes without that user's consent;
    c) using data collected from a user pursuant to TACT for a purpose other than facilitating contact tracing for the immediate public health purpose or implementing TACT system improvements; and
    d) reidentifying or attempting to reidentify deidentified, anonymized, or aggregated data collected pursuant to TACT.

9) Defines core terms, including the following:

a) "consent" means an affirmative act by an individual that clearly and conspicuously communicates the individual's authorization of an act or practice and is made in the absence of any mechanism in a user interface that has the purpose or substantial effect of obscuring, subverting, or impairing decisionmaking or choice to obtain consent;
b) "data" means measurements, transactions, determinations, locations, or other information, whether or not that information can be associated with a specific natural person;
c) "personal information" means data that identifies, relates to, describes, is reasonably capable of being associated, or could reasonably be linked, directly or indirectly, with a specific natural person or household;
d) "public health entity" means a state or local health department or a public university health center; and
e) "business" means a sole proprietorship, partnership, corporation, association, or other group, including, but not limited to, a nonprofit entity.

COMMENTS

1. What is contact tracing?

According to the Centers for Disease Control and Prevention (CDC):

> Contact tracing is used by health departments to prevent the spread of infectious disease. In general, contact tracing involves identifying people who have an infectious disease (cases) and people who they came in contact with (contacts) and working with them to interrupt disease spread. This includes asking people with COVID-19 to isolate and their contacts to quarantine at home voluntarily.

This process typically entails the following elements:

- Interviewing people with COVID-19 to identify everyone they had close contact with during the time they may have been infectious;
- Notifying contacts of their potential exposure;
- Referring contacts for testing;
- Monitoring contacts for signs and symptoms of COVID-19; and/or
- Connecting contacts with services they might need during the self-quarantine period.

On May 22, 2020, Governor Newsom announced the launch of California Connected, which he hailed as "the state's comprehensive contact tracing program and public awareness campaign."[2] The program was detailed as follows:

> As part of California Connected, public health workers from communities across the state will connect with individuals who test positive for COVID-19 and work with them, and people they have been in close contact with, to ensure they have access to confidential testing, as well as medical care and other services to help prevent the spread of the virus.
>
> The state's program is led by the Administration in collaboration with the California Department of Public Health, local public health departments and the University of California, San Francisco (UCSF) and Los Angeles (UCLA), which have launched a robust online training academy to develop a culturally competent and skilled contact tracing workforce.

2. Assessing the security and privacy concerns surrounding contact tracing

The Governor's Office has assured the public that the data is only collected and stored for use by local and state public health departments for public health purposes and that public health authorities would not share information collected as part of these contact tracing efforts with any outside entities.[3]

Despite these commitments to protecting privacy, there is arguably a void of regulations and protections for how contact tracing can be carried out, who can engage in contact tracing, and what can be done with the information collected. Concerns about this gap are only amplified when new technologies are incorporated into contact tracing efforts and when entities outside of public health departments, including law enforcement and private entities, are conducting the tracing.

Many countries and other states have introduced apps to trace the spread of COVID-19 only to be met with a landslide of complaints and concerns surrounding the security and confidentiality of this technologically-assisted contact tracing.[4] Officials in these jurisdictions were forced to scramble to "address serious complaints that soon arose over extensive user data-mining or poor security practices." Warnings streamed in from

---

[2] Office of Governor Gavin Newsom, *Governor Newsom Launches California Connected – California's Contact Tracing Program and Public Awareness Campaign* (May 22, 2020) Press Release, https://www.gov.ca.gov/2020/05/22/governor-newsom-launches-california-connected-californias-contact-tracing-program-and-public-awareness-campaign/ [as of Aug. 5, 2020]. All further Internet citations are available as of August 9, 2020.
[3] *Ibid.*; California Connected, *Contact Tracing* (August 3, 2020) https://covid19.ca.gov/contact-tracing/.
[4] Natasha Singer, *Virus-Tracing Apps Are Rife With Problems. Governments Are Rushing to Fix Them* (July 8, 2020) The New York Times, https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html.

human rights groups and technologists that "the design of many apps put hundreds of millions of people at risk for stalking, scams, identity theft or oppressive government tracking — and could undermine trust in public health efforts."

Studies have found that many of the apps being used lacked basic protections for the data and required or accessed sensitive personal information from users. Google and Apple have led the charge with the development of sophisticated tracing technology that principally relies on Bluetooth technology and importantly does not rely on GPS data, which can pinpoint a person's exact locations. However, some countries have been dismayed to learn that Google's Android system, the most popular in the world, requires users of the apps developed with the technology to "first turn on the device location setting, which enables GPS and may allow Google to determine their locations."[5]

The core concern with this sort of contact tracing is that the apps can continuously collect sensitive data about users, including health information, precise location data, and the social interactions of the person. While this may provide a richer set of data for officials, it comes with serious privacy and security risks without proper oversight and regulation. Establishing oversight and regulation not only addresses the identified privacy and security risks but also builds the public trust that is necessary for effective contact tracing. Recent studies show that effective regulation can make individuals more likely to download a contact tracing app, share information about their contacts, and change their behavior.

For instance, a recent Axios-Ipsos poll found that a large majority of Americans report they would likely follow core elements of contact tracing systems.[6] Eighty-four percent said they would be likely to self-quarantine if they were notified that they came into contact with a coronavirus-infected individual, and 76 percent said they would give officials a list of all the people with whom they had recently come into contact. However, those numbers dropped significantly when it required access to their cell phone location data. The report concluded that "[f]ew Americans are likely to opt-in to cell phone-based contact tracing systems at this time." Specifically, the report found that only 33 percent would be likely to opt-in to a cell phone based contact tracing system established by major tech companies. The number only rose to 51 percent for such a system sponsored by the CDC.

---

[5] Natasha Singer, *Google Promises Privacy With Virus App but Can Still Collect Location Data* (July 20, 2020) The New York Times, https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html.

[6] Chris Jackson & Mallory Newall, *Axios-Ipsos Coronavirus Index*, (August 4, 2020) Ipsos, https://www.ipsos.com/en-us/news-polls/axios-ipsos-coronavirus-index.

A recent Kaiser Family Foundation survey found that over 60 percent were willing to download a contact-tracing app if managed by their state or local health department.[7] But the latter study similarly found a much lower adoption rate, 31 percent, was likely if managed by a private tech company. The study concluded that while there is generally strong willingness to download the app, the public is extremely divided when certain types of information, such as geolocation information, is collected.

Highlighting the importance of these studies and appropriately responding to them, research out of Oxford University shows that digital contact tracing could "stop the epidemic if approximately 60% of the whole population use the app and adhere to the app's recommendations."[8] However, it made clear that lower percentages will also have a positive effect. Regardless of the necessary or ideal participation rate, the experts seem clear that trust is absolutely critical. The responses in the studies above, among others, reveal that the confidence of individuals hinges greatly on who is collecting the data, what data is being collected, and what can be done with that information.[9] Professor Michael Parker, a senior ethicist at Oxford University's Nuffield Department of Population Health, and an author of the study discussed above, acknowledges the legitimate "concerns relating to the potential misuse of data" and stresses that individuals need "to feel confident that these issues have been taken seriously."[10] Professor Christophe Fraser, co-lead on the contact tracing program at Oxford University's Nuffield Department of Medicine and an independent scientific advisor to the UK government's contact tracing efforts, puts a finer point on the issue:

> We know that public health is all about building trust. So how do we build an environment where people know that the data is being shared for good? People fear misuse of data, which we've seen in the digital space. How do we stop misuse while encouraging positive use of data? This is clearly an important area. The power to do good things increases as we share information, but we need frameworks.[11]

---

[7] Ashley Kirzinger et al., *KFF Health Tracking Poll – Late April 2020: Coronavirus, Social Distancing, and Contact Tracing* (April 24, 2020) Kaiser Family Foundation, https://www.kff.org/coronavirus-covid-19/issue-brief/kff-health-tracking-poll-late-april-2020/.

[8] *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown* (April 16, 2020) University of Oxford, https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

[9] Ashley Kirzinger et al., *KFF Health Tracking Poll – Late April 2020: Coronavirus, Social Distancing, and Contact Tracing* (April 24, 2020) Kaiser Family Foundation, https://www.kff.org/coronavirus-covid-19/issue-brief/kff-health-tracking-poll-late-april-2020/; Chris Jackson & Mallory Newall, *Axios-Ipsos Coronavirus Index*, (August 4, 2020) Ipsos, https://www.ipsos.com/en-us/news-polls/axios-ipsos-coronavirus-index.

[10] *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown* (April 16, 2020) University of Oxford, https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

[11] Patrick Howell O'Neill, *No, coronavirus apps don't need 60% adoption to be effective* (June 5, 2020) MIT Technology Review, https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download.

The author of this bill asserts that the research makes clear that "sufficient protections for privacy, including consent requirements and data use limitations, must be in place for widespread use of TACT to be effective in combatting COVID-19 and future public health emergencies." As will be discussed, this bill attempts to regulate these aspects of TACT.

3. Filling the gap

This bill works to address the privacy and security concerns inherent in this type of data collection and dissemination. It governs "technology-assisted contact tracing" (TACT), defined as:

> the use of a digital application or other electronic or digital platform that is capable of independently transmitting information and is offered to individuals for the purpose of identifying and monitoring individuals, through data collection and analysis, who may have had contact with an infectious person as a means of controlling the spread of a communicable disease.

The bill specifically exempts devices issued at specified health facilities, such as electronic key cards, from the definition of TACT where such devices are only used within the issuing facility's campus.

While various health information laws, such as HIPAA and CMIA, regulate the collection and maintenance of medical information, the coverage is limited and does not provide adequate protections in the contact tracing sphere, leaving a significant legal gap guiding such programs. This bill implements various requirements and protections in connection with technology-assisted contact tracing.

a. Consent and control

A core principle of the bill is that users must clearly and intelligently consent to the collection, use, disclosure, and retention of their personal information. The bill provides a robust definition of "consent," requiring an affirmative act by the user that "clearly and conspicuously communicates" the user's authorization of an act or practice and that is made "in the absence of any mechanism in a user interface that has the purpose or substantial effect of obscuring, subverting, or impairing decisionmaking or choice to obtain consent."

This consent would be illusory if it could be coerced. Therefore, the bill prohibits businesses or public entities from mandating participation in TACT or discriminating against or penalizing users based on their participation or nonparticipation in TACT, or any behavior or disclosure pursuant thereto. Public health entities are also prohibited from charging any fees for participation in TACT.

The bill also affords users a measure of control over their data. It requires public and private entities to provide users a mechanism to access, correct, and delete their personal information and a mechanism to revoke any previously provided consent. Users must also be given a clear and simple process for disabling or removing TACT. These provisions not only engender trust in communities, but they better ensure the integrity of the systems and the reliability of the data collected. It should be noted that the reliability of the data is also enhanced through the requirement that "any report of exposure, including a presumptive report of exposure, be verified by a health care professional or public health entity before notifying persons who have been or may have been in contact with the reporting individual or before publicly disclosing exposure data."

b. Transparency and oversight

Many of the TACT programs that have been deployed have been derailed by revelations of personal information that was being collected unbeknownst to users or the entities deploying the technology. Ultimately, trust is critical to ensuring effective contact tracing, and full disclosure about what information is being collected and what is done with it is crucial to establishing that trust.

This bill provides that any public health entity or business that offers TACT must provide meaningful disclosures and get a user's buy in before deploying the technology. Specifically, these entities must disclose the categories of data being collected and the public health purpose for which the user's data will be collected, used, maintained, or disclosed, and to whom that data will be disclosed when seeking their affirmative consent.

In addition, the public health entity or business must also publicly issue a report at least every quarter that details the number of users whose personal information was collected, used, or disclosed pursuant to TACT; the categories of data collected, used, or disclosed and the specific public health purposes for which each category was collected, used, or disclosed pursuant to TACT; and the recipient to whom any of the information was disclosed.

A TACT contract between a public health entity and a business must also include certain transparency measures. The business is required to provide any source code created by the business pursuant to the TACT contract to both the public health entity and the entity charged with oversight of the public health entity's acquisitions. These transparency measures instill trust in the program and foster accountability.

c. Appropriate and adequate safeguards

As learned from countless examples around the world, the security of these programs is paramount. The bill requires a business or public health entity to implement and

maintain reasonable security procedures and practices to protect the data collected from unauthorized use, disclosure, access, destruction, or modification. This includes administrative, physical, and technical safeguards be put into place. Furthermore, any data collected and maintained pursuant to TACT must be encrypted to the extent practicable.

The security of these systems is also enhanced by requiring businesses and public health entities to limit the data that is collected, used, maintained, or disclosed to only that which is "reasonably necessary to provide TACT services." TACT contracts must also prohibit a contractor from collecting data that is not "directly necessary for the public health purposes enumerated in the contract." The bill also specifically bans a public health entity from offering TACT that collects, uses, retains, or shares geolocation information. Privacy issues arise anytime geolocation information is being systematically collected, used, and disclosed. Given the effectiveness of other models, including those relying on Bluetooth technology, highly sensitive geolocation information is largely unnecessary. It also exposes users to additional risks and opens the door for misuse of the information. As highlighted in the studies discussed above, users are also less likely to engage in contact tracing if they know that geolocation information is being collected.

Furthermore, the bill restricts contractors from maintaining any data collected pursuant to a TACT contract after the termination or expiration of the contract. It also requires businesses and public health entities to delete personal information collected pursuant to TACT within 60 days of collection.

"Data" is defined as measurements, transactions, determinations, locations, or other information, whether or not that information can be associated with a specific natural person. "Personal information" is defined as data that identifies, relates to, describes, is reasonably capable of being associated, or could reasonably be linked, directly or indirectly, with a specific natural person or household. The latter definition tracks the definition of personal information in the CCPA. Concerns have been raised that the deletion requirement should be extended to cover all "data" rather than just "personal information," given the reality that even deidentified information can be connected back to users.

In response, the author has amended the bill to require the deletion of any other data collected pursuant to TACT within 60 days with a limited exception for data that is maintained and used solely for purposes of research, as specified. The bill therefore requires the deletion of *all* personal information and further requires the deletion of data not considered personal information, with a limited exception.

The bill's data minimization component and expanded deletion requirement significantly limit the exposure of personal information to theft and misuse.

d. Limiting who can properly engage in TACT

Traditionally, public health departments have been the sole entities taking the lead on contact tracing efforts. However, the widespread pandemic currently consuming the world has brought in a multitude of players. In order to ensure the proper implementation of TACT, the bill lays out various restrictions and requirements.

First, the bill restricts public entities other than public health entities from entering into a TACT contract at all. The bill defines a "public health entity" as "a state or local health department or a public university health center." The bill further restricts a public health entity that is a public university health center from allowing access to TACT data by any agent or division of the university outside of the health center. This ensures that only those public entities that have been officially and primarily tasked with supporting public health are engaging in this process.

While private entities are not restricted from engaging in TACT without public health entity involvement, they are required to clearly and conspicuously disclose that they are not affiliated with a public health entity and are prohibited from misleadingly holding themselves out as being so affiliated. A certain amount of credibility is afforded to private entities that engage in contact tracing in affiliation with a public health entity. This bill requires that such private entities be contractually required to abide by many of the provisions discussed herein. In fact, except for the public reporting requirement, such private contractors must be contractually obligated to comply with the requirements imposed on public health entities.

Such contracts between public health entities and businesses must also include clear performance metrics to ensure the effectiveness of the systems and cannot extend beyond one year. Certain security requirements must also be written into these contracts, establishing clear use limitations and subjecting them to data breach notification requirements.

e. Preventing misuse

One of the primary privacy concerns with TACT, outside of the threat of unauthorized data exfiltration, is that the data collected can be used for other purposes outside of directly battling the underlying public health emergency. Effective contact tracing requires the widespread collection of, at times, sensitive personal information from individuals. However, the process is undermined and trust is broken if that data can be used for other purposes or combined with other data. For example, it is arguably a problematic practice, and a breach of a user's reasonable expectations, to allow such information to be used for other business purposes, such as profiling consumers or marketing to them, or for the information to be provided to other public entities, including federal authorities, for any purposes other than stemming the spread of a communicable disease.

This bill establishes various safeguards in response to such concerns. First, public health entities and businesses working with public health entities are prohibited from using certain data for anything "other than facilitating the response to the immediate public health purpose," or TACT system improvements carried out by the business. The bill makes clear that "facilitating the response to the immediate public health purpose" does not include "enforcement of laws or orders pertaining to the public health purpose or created in response to the public health purpose, or investigations into violations of those orders and laws." Similarly, businesses participating in TACT outside of an affiliation with public health entities are restricted from "using data collected from a user pursuant to TACT for a purpose other than facilitating contact tracing for the immediate public health purpose or implementing TACT system improvements."

TACT contracts must also restrict contractors from disclosing the data to any person or entity without the express written consent of the public health entity and the affirmative consent of the individual whose data would be disclosed. The bill also prohibits all businesses from reidentifying or attempting to reidentify deidentified, anonymized, or aggregated data.

All businesses and public entities are restricted from associating data collected from a user pursuant to TACT in any way with data otherwise collected or maintained for other purposes. However, the bill does allow a business not affiliated with a public health entity to so associate data with the user's consent. It should be noted that, as discussed above, this would have to be affirmative consent from the user and the business would have to clearly disclose the purposes to which the data would be used. As noted in the letter submitted by a coalition of consumer and privacy groups: "Combining data sets generates more detailed individual profiles, and carries heightened privacy risks." TACT contracts are also required to prohibit contractors from using data collected for a commercial purpose or to obtain anything of value apart from due compensation pursuant to the TACT contract.

To ensure the public health entity maintains control, the bill provides that any "data collected by, and any inventions, discoveries, intellectual property, technical communications, and records originated or prepared by, the contractor in the course of activities governed by the contract, including papers, reports, charts, computer programs, and other documentation, shall be the public health entity's exclusive property."

f. Enforcement

Many believe that a right without a remedy is no right at all. The bill was recently amended to include a tiered system of enforcement in order to appropriately calibrate the enforcement to the violation. Businesses in violation of the bill's provisions are subject to a civil judgment for injunctive relief, reasonable attorneys' fees, and actual or statutory damages. The damages progress if the violation results in the disclosure of

data and/or the violation is willful. Such civil actions can be brought by public prosecutors or members of the public.

Public entities in violation are also subject to a similar tiered enforcement scheme, however, members of the public are only authorized to bring an action for injunctive relief, to stop the unlawful conduct, and reasonable attorneys' fees.

These enforcement mechanisms will make compliance more likely, further protecting privacy and building public trusts. This in turn makes the state's contact tracing efforts more likely to succeed.

4. Stakeholder positions

According to the author:

> AB 1782 would comprehensively regulate the development and use of technology-assisted contact tracing (TACT) applications and platforms by public and private entities, including specifying that any public or private TACT service must obtain affirmative consent before collecting any user's data and abide by stringent limitations on the collection, maintenance, use, and disclosure of data. Importantly, AB 1782 would also prohibit discrimination on the basis of participation in TACT and specify that the provisions of the bill apply to employees as well. By providing explicit protections for user data collected, used, and disclosed by TACT services, AB 1782 would protect individual privacy and increase public confidence in promising digital techniques for combating the spread of COVID-19 and other infectious diseases.
>
> The California Constitution considers the right to privacy inalienable. As technology changes the nature of disease response, it is imperative that we honor this right by ensuring that individual privacy is protected when technology is used for public health purposes. Broad public participation in TACT is essential for effectiveness in combatting COVID-19 and future public health threats, and public confidence in data privacy and security is critical to driving that participation. This bill would provide the public with the confidence necessary to contribute to this greater good.

Writing in support, the California Immigrant Policy Center asserts that "it is imperative that the state demonstrate its commitment to ensuring the privacy of all Californians." They argue the bill "will help ease concerns around contact tracing and encourage more families to get tested for COVID-19, regardless of immigration status."

A coalition of industry and technology groups write in opposition to the bill. They argue the bill "conflicts with CDC guidelines, existing law, and proposed legislation,

thus causing confusion and creating a lack of coordination amid this pandemic." Specifically, they assert that the definition of TACT is vague and overbroad and that the bill "arguably conflicts with current employment laws."

The coalition also raises objections to providing users the ability to refuse to participate in TACT and claim that the anti-discrimination provisions "deny any organization, government or private, from mitigating risks to consumers and employees for individuals who refuse to participate in TACT."

It should be noted that the anti-discrimination provisions are in connection with a user's decision of whether to participate in contact tracing done through technology-assisted means and does not control a business or public health entity's ability to implement proper public health measures unconnected to that specific decision or to otherwise interfere with a business' or public health entity's ability to comply with legal requirements. The author has also committed to continuing to work with this Committee and stakeholders to address issues regarding employers' ability to impose reasonable practices as recommended by public health officials.

AARP California writes in support of the bill. It discusses the development and deployment of TACT programs and states:

> Given the urgency with which such programs need to be deployed and given the complexity and far reaching impacts of the technological and programmatic choices that have to be made, it is imperative that a set of policies and accompanying regulation be defined to address these considerations so that these programs are developed in a manner consistent with the parameters necessary for public acceptance and protection.
>
> AB 1782 provides this necessary regulation and guidelines for California.

A coalition of consumer and privacy groups writes in support of a previous version of the bill. They note that the bill contains important privacy safeguards, specifically highlighting how critically important the provisions are that require affirmative consent, systematic purging, and data minimization. However, they also urge the author to amend the bill to include stronger and more robust protections. A number of the suggested provisions have been included, at least in part, through recent amendments to the bill.

SUPPORT

AARP
ACLU California
California Immigrant Policy Center

Common Sense Media
Consumer Federation of America
Electronic Frontier Foundation
Privacy Rights Clearinghouse

OPPOSITION

California Business Properties Association
California Chamber of Commerce
California Manufacturers & Technology Association
California Retailers Association
Civil Justice Association of California
CompTIA
Consumer Technology Association
Insights Association
Internet Coalition
National Payroll Reporting Consortium
Personal Insurance Federation of California
Silicon Valley Leadership Group

RELATED LEGISLATION

Pending Legislation:

AB 660 (Levine, 2020) prohibits law enforcement from engaging in any contact tracing and prohibits the use of contact tracing information except for contact tracing purposes. This bill is set to be heard by this Committee on August 13, 2020.

AB 685 (Reyes, 2020) requires employers to provide specified notifications to employees and specified state entities when they are aware of the exposure of their employees to COVID-19. This bill is currently in the Senate Appropriations Committee.

Prior Legislation: None known

PRIOR VOTES:

This bill was recently gutted and amended. As such, all prior votes on the bill are irrelevant.

****