ASSEMBLY THIRD READING
AB 814 (Levine)
As Amended May 24, 2021
Majority vote

SUMMARY

Prohibits any data collected, received, or prepared for purposes of contact tracing from being used, maintained, or disclosed for any purpose other than facilitating contact tracing efforts, and would require this data to be deleted within 60 days, unless it is in the possession of a state or local health department. The bill additionally prohibits law enforcement, as defined, from engaging in contact tracing,

Major Provisions

1) Prohibits any data collected, received, or prepared for purposes of contact tracing from being used, maintained, or disclosed for any purpose other than facilitating contact tracing efforts.

2) Requires all data all data collected, received, or prepared for purposes of contact tracing to be deleted within 60 days, except for data in the possession of a local or state health department.

3) Prohibits any officer, deputy, employee, or agent of a law enforcement agency from engaging in contact tracing, except that it authorizes an employee of a law enforcement agency to conduct contract tracing of employees within the same law enforcement agency

4) Clarifies that the above provisions shall not apply to data used, maintained, or disclosed by an employer to the extent that the use, maintenance, or disclosure of that data is necessary to comply with a state or federal workplace health and safety law or regulation.

5) Authorizes a person to bring a civil action seeking injunctive relief and reasonable attorneys' fees for any violation of the provisions above.

6) Defines "contact tracing" to mean 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.

COMMENTS

Ensures personal information collected for public health purposes is only used for that purpose: This bill prohibits any data collected, received, or prepared for purposes of contact tracing from being used, maintained, or disclosed for any purpose other than facilitating contact tracing efforts. The bill broadly defines data to mean "measurements, transactions, determinations, locations, or other information, whether or not that information can be associated with a specific natural person" and defines contact tracing as "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."

Taken together, these definitions mean that even deidentified data, the type of data that normally evades privacy laws, would be regulated by this bill so long as it was collected as a means to control the spread of a communicable disease. The bill also makes no distinction between public or private actors, meaning that this prohibition would apply to contact tracing by the government

and employers/commercial entities alike. While traditionally contact tracing has been conducted by the government, new technologies made contact tracing easily accessible to employers, many of whom sought to require employees to download "exposure notification applications" on their mobile phones in this past year.

This bill creates a statutory framework for protecting contract tracing data, which would apply to both traditional contact tracing and contact tracing technology, and both the public and private sector. It would strictly limit how contact tracing data may be used and also require that data be deleted after 60 days, unless that data is held by a public health department.

Prohibits law enforcement from contact tracing: Traditionally, contact tracing is conducted through interviews of infected individuals to collect information regarding with whom they have come into contact since infection, and the nature of those contacts. Contacts deemed to be at risk of infection are then advised to take certain actions, such as testing and self-isolation, to avoid further transmission.

Contact tracing can be highly effective depending on the nature of the illness, particularly in situations in which an individual becomes contagious before they present symptoms. However, traditional contact tracing demands a robust workforce of trained personnel, and suffers from imperfect recollection and a long latency between initial reports of infection and action taken on the part of those at risk. To address these challenges over the past year, some rural counties turned to law enforcement to assist in contact tracing efforts.

Specifically, news of Madera County's use of the sheriff's department for contact tracing last year coincided with news of some local governments sharing the names and/or addresses of people who had tested positive for COVID-19, and other reports throughout the country of local governments looking into relatively untested ways of tracking the spread of COVID, such as facial recognition technology, geolocation tracking, and fever detection cameras. Additionally, in January of this year, a local newspaper reported that San Diego County had been releasing the addresses of COVID positive individuals to law enforcement for over nine months, while at the same time refusing to release public data that might provide insight into where the outbreaks in that county had happened.

Reports such as these have seemingly undermined the public's trust in government and have blurred the lines between public health and law enforcement. Sharing the medical data and addresses of people who test positive likely created a chilling effect causing some people to avoid getting tested. Specifically, there is a concern that vulnerable populations such as homeless or undocumented individuals may not be willing to get tested if they fear their information will ends up in the possession of law enforcement. Californians have a constitutionally protected right to privacy, and these practices arguably undermine a very basic tenant of privacy: when the government collects sensitive information about individuals for one purpose, it should not use that data for another purpose.

To promote public trust, this bill prohibits law enforcement from conducting contact tracing, subject to a narrow exception. Specifically, given the massive COVID outbreaks within correctional facilities in California, recent amendments ensure that this bill importantly allows law enforcement agencies to conduct contact tracing of their own employees.

Enforcement: This bill allows an individual to bring a civil action for a violation of this bill for injunctive relief, and requires the court to grant any prevailing plaintiff reasonable attorney fees.

As a general matter, laws without adequate enforcement mechanisms do little to protect the individuals they were intended to serve because individuals either lack a statutory mechanism by which to seek relief, or litigating a claim is cost prohibitive. It is important to note that money damages are not available for a violation of this bill's provisions. The bill instead would allow an individual to ask the court to order that a person or entity engage in or stop a specified act. Importantly, the bill would require a court to grant a prevailing plaintiff reasonable attorney fees, which should allow individuals with insufficient means to pay-out-of-pocket for an attorney to still obtain legal counsel on a contingency basis.

According to the Author

> One of the primary concerns about contact tracing, outside of the threat of unauthorized data breaches, is that the data collected can be used for other purposes outside COVID-19 prevention efforts. Research shows that when individuals know their public health department is managing an app for contact tracing rather than a private technology company, they are more likely to participate. The public trusting the entity that conducts contact tracing is critical to maximizing participation to effectively prevent community spread of the virus. Despite commitments to protecting privacy, there is a lack of regulations and protections for the very new practice that has become critical so quickly. There have been cases including in Madera County where various law enforcement agencies are conducting contact tracing in their community. Immigrant communities, especially undocumented immigrants and communities of color are less likely to interact with law enforcement, regardless the purpose. AB 814 prohibits law enforcement employees from engaging in contact tracing and builds safeguards to protect Californians' personal information [so that it is] used only for contact tracing purposes.

Arguments in Support
A coalition of six organizations dedicated to protecting consumer privacy including the American Civil Liberties Union, Electronic Frontier Foundation and the Consumer Federation of America writes in support that this bill includes important privacy protections, described as follows:

> If a company collects a person's personal data while acting as a government contractor for contact tracing purposes, AB 814 would stop that company from using it to target its own ads or selling it to a data aggregator. And if a public health agency collects the same data, AB 814 would stop them from transferring it to police or immigration officials. These protections support California's pandemic response by addressing real concerns that would prevent some Californians from being willing to speak to contact tracers.
>
> […]
>
> [T]his [also] bill sets a 60-day deadline to purge data collected for purposes of contact tracing (with an exception for state and local health departments). See Sec. 601(b). COVID-19 has a 14-day incubation period, so older information will not aid in addressing the current crisis. But that stale information can still be stolen, misused, and harnessed for inappropriate purposes.

Arguments in Opposition
A coalition of organizations including the California Chamber of Commerce, the Civil Justice Association of California, and the California Grocers Association, among others, oppose this bill

unless amended to address a number of concerns. The coalition argues that the bill is overly broad in that it would "prohibit the use of data that was not solely collected, received, or prepared for [contact tracing]. AB 814 applies to all forms of contact tracing, even if just a pen and paper are used. For example, if sign-in sheets were "collected" for purposes of building security, but were later "received, or prepared" for purposes of contact tracing, then AB 814 would end up banning the use of sign-in sheets, or any other information for that matter, which may not be collected exclusively for the purpose of contact tracing."

The coalition also contends that "if an employer asks an employee to write their phone number on a contact tracing form, that information is now swept into the definition of 'data collected, received or prepared for contact tracing.' However, the employer has the employee's phone number in numerous files and for several reasons other than contact tracing."

The coalition also argues that the requirement to delete data collected for contact tracing is in "direct conflict with existing law." In support of this contention, the letter describes how data collected for contact tracing may be useful, by stating that there "are legitimate and important reasons why this information should not be deleted, including tracking the effectiveness of treatment; anticipating hot spots; or identifying whether specific communities are more impacted than others. With this definition, this information will be swept into what is considered contact tracing data and be required to be deleted within 60 days." Importantly, the coalition notes that "Cal OSHA's recent Guidance sets forward strict obligations for recording and reporting occupational injuries and illnesses for employees who contract COVID-19. California employers must record specific work-related COVID-19 illnesses on their Log 300s and keep those log 300s for 5 years in some instances and 30 years in others."

FISCAL COMMENTS

According to the Assembly Appropriations Committee:

> Possible cost pressures (Trial Court Trust Fund) in the low hundreds of thousands of dollars in increased workload to the extent this bill creates a new civil action for injunctive relief. One hour of court time costs approximately $956. If 20 requests for injunctive relief are filed statewide requiring an average of 12 hours of court time each, the cost to the courts would be $229,440.
>
> Although courts are not funded on the basis of workload, increased pressure on the Trial Court Trust Fund and staff workload may create a need for increased funding for courts from the General Fund (GF) to perform existing duties. This is particularly true given that courts have delayed hundreds of trials and civil motions during the COVID-19 pandemic resulting in a serious backlog that must be resolved. The Governor's 2021-22 budget proposes $72.2 million dollars in ongoing GF revenue for trial courts to continue addressing the backlog of cases in order to provide timely access to justice.

VOTES

ASM PRIVACY AND CONSUMER PROTECTION: 10-1-0
YES: Chau, Bauer-Kahan, Bennett, Carrillo, Cunningham, Gabriel, Gallagher, Irwin, Lee, Wicks
NO: Kiley

ASM JUDICIARY: 8-2-1
YES: Stone, Chau, Chiu, Lorena Gonzalez, Holden, Kalra, Maienschein, Reyes
NO: Davies, Smith
ABS, ABST OR NV: Kiley

ASM APPROPRIATIONS: 12-4-0
YES: Lorena Gonzalez, Calderon, Carrillo, Chau, Gabriel, Eduardo Garcia, Levine, Quirk, Robert Rivas, Akilah Weber, Holden, Luz Rivas
NO: Bigelow, Megan Dahle, Davies, Fong

UPDATED

VERSION: May 24, 2021

CONSULTANT: Nichole Rocha / P. & C.P. / (916) 319-2200 FN: 0000758