# Three CCPA Implications of Business Screening for COVID-19

**In Brief:**

- Covered businesses taking employees' temperatures, or requiring customers or employees to report COVID-19 symptoms must provide an appropriate privacy notice at or before the point of collection.
- Collecting such data may ultimately require the business to update its public-facing privacy policy, which must disclose all categories of personal information collected within the past 12 months.
- Collecting biometric data (such as body temperature) and other personal health information exposes the business to a greater risk of being sued in the event of a data breach. Plan to restrict access, limit retention, and securely dispose of the data once it's no longer needed.

## In Depth:

The tension between privacy rights and public safety isn't new, but COVID-19 and the California Consumer Privacy Act ("CCPA") are. On January 1, 2020, just as the novel coronavirus was beginning its global migration, the CCPA took effect, ushering in a new era of data privacy regulation in the United States. On March 26, 2020, California's Attorney General rejected calls to postpone his office's enforcement of the CCPA due to the outbreak's impact on many covered businesses, so enforcement will begin as planned by July 1, 2020. Companies doing business in California have good reason to be proactive in protecting the well-being of their employees and the safety of the workplace during this pandemic, but in doing so they should remain mindful of how the CCPA may impact some of those efforts. This is especially true for those companies who meet the CCPA's definition of a covered "business" because their annual revenues exceed $25 million; or they annually receive or share the personal information of 50,000 or more California residents, households, or devices; or at least 50% of their annual revenue comes from selling California residents' personal information.

*1. Collection of personal information from California consumers or employees requires notice at the right time and place.*

Some businesses providing essential services during the pandemic, and businesses whose employees may start returning to the office in a matter of weeks or months, may consider taking employees' body temperatures as a condition of entering the workplace each day. Businesses whose personnel go to customers' homes to provide services may consider asking customers to disclose in advance whether any members of the household have exhibited COVID-19 symptoms. These measures, and others like them, may be prudent in the context of a global pandemic, and the CCPA doesn't prohibit them. It does, however, require timely notice to impacted individuals who are California residents.

An individual's body temperature is a form of biometric data, which the CCPA explicitly identifies as a category of personal information. An individual's COVID-19 status constitutes medical information, another protected category. Under the CCPA, a covered business must provide written notice "at or before" the point of collection, disclosing the categories of personal information collected and the purposes for which they will be used. Businesses must be mindful that collection of unique health information carriers unique notice obligations, and failure to meet those obligations may trigger enforcement action by the attorney general, which can result in monetary penalties of up to $7,500 per incident, not to mention reputational damage.

*2. Collection will likely require updating your Privacy Policy.*

Separate from the obligation to provide notice at collection is the business's obligations to post a Privacy Policy, which under the CCPA must disclose both online and offline collection of personal information (among other things). So collection of biometric data, or any other personal information, in person has Privacy Policy implications under CCPA. For example, the Privacy Policy must disclose categories of personal information collected within the past 12 months. So if a business starts requiring California consumers to disclose their COVID-19 status as a pandemic-specific safeguard, then ends the practice in July 2020, the business's Privacy Policy must disclose collection of "biometric data" through at least July 2021 in order to satisfy the 12-month "look back" requirement.

Businesses requesting household-specific COVID-19 status in advance of a service visit must still treat the response as personal information, even though it is not necessarily tied to a particular individual. That's because the CCPA defines personal information broadly to include information that "could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(o)(1) (emphasis added.)

3. Collecting biometric data or medical information increases the risk of being sued in the event of a data breach, so mitigate accordingly.

The CCPA allows consumers to sue for statutory damages of up to $750 per consumer, per incident, when unencrypted and sensitive categories of personal information are subject to unauthorized access and removal due to a business's violation of the duty "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Those sensitive categories are set forth in California's information security law, Civil Code § 1798.81.5, which was recently amended to add biometric data to a list that already included medical information. As a result, a business's collection of body temperature or medical information for the first time during a pandemic may result in new exposure to consumer litigation.

In addition to biometric data and medical information, the categories of personal information that can trigger consumer litigation under the CCPA if breached include social security number, driver's license or other government-issued ID number, health insurance information, and financial or online account login credentials. See Cal. Civil Code § 1798.81.5, 1798.150. To help minimize exposure, businesses who collect one or more of these categories should, among other things, apply modern encryption to the greatest extent feasible, restrict who has access to the data, and take steps to ensure that the data is securely deleted, or at least irreversibly anonymized, once it is no longer needed. Indeed, in discussing the Attorney General's response to an open letter requesting postponement of CCPA enforcement until after the COVID-19 crisis subsides, an advisor to the Attorney General was quoted as "encourag[ing] businesses to be particularly mindful of data security in this time of emergency."[1]

## Authors:

Travis P. Brennan
949.725.4271
tbrennan@sycr.com

Ahmad Takouche
949.725.4153
atakouche@sycr.com

1 https://www.forbes.com/sites/martyswant/2020/03/19/citing-covid-19-trade-groups-ask-californias-attorney-general-to-delay-data-privacy-enforcement/#668b73e15c30.