Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Should Consumer Data Privacy Laws Apply To The Gov't?

By **Mark Lyon, Cassandra Gaedt-Sheckter and Arjun Rangarajan**
(June 7, 2019, 11:59 AM EDT)

Mark Lyon

Cassandra Gaedt-Sheckter

Arjun Rangarajan

A general human right to privacy may not be explicit in the United States, but there is a foundational expectation of the sanctity of one's personal effects; for example, the Fourth Amendment of the U.S. Constitution prevents the government from conducting unreasonable searches and seizures, and was grounded in disdain for abuse by the pre-revolutionary British government. In the 21st century, in which information can be every bit as valuable as personal possessions, should similar protection from government intrusion apply to electronic consumer data?

The California Consumer Privacy Act is slated to become effective Jan. 1, 2020, and is California's attempt at protecting the privacy of its citizens through a comprehensive law. Although the CCPA likely will be modified (several amendments are currently pending in the Legislature), it appears that government entities will be exempt from its clutches: the CCPA applies only to "businesses" that are "organized or operated for the profit or financial benefit of [their] shareholders or other owners." Governments do not fit that definition.

That is not to say that governments do not routinely collect personal data, or that privacy laws should not apply to them. In some cases, governments are bound by privacy requirements related to the specific collection of data. For example, Title 13 of the United States Code prohibits the U.S. Census Bureau from publishing personal information of individuals. And recently, the Census Bureau has been working with scholars to modernize their data practices in order to ensure that the results of the decennial census in 2020 will be released with differential privacy protections for individuals.

Similarly, there are state-specific privacy laws — such as those applying to state agencies, like the California Department of Motor Vehicles — consistent with the United States' patchwork approach to privacy law. However, there is no overarching privacy regulation that addresses the government's use of all types of personal data from its citizens.

But governments are increasingly entering into the business of utilizing consumer data like any other private entity, potentially causing interesting debates relating

to discrimination, consumer privacy requests, “anonymized” data and data that is made publicly available by the government. Take the current example of trip data from electronic scooters. Cities across the country are mandating that shared mobility companies provide scooter data, including location and trip data.

For example, in March of this year, the Los Angeles Department of Transportation only gave year-long permits for the operation of scooters in Los Angeles where the companies agreed to share location and trip data of the scooters, including vehicle identifier, provider name, trip time and trip cost, and a vehicle endpoint telemetry that is accessed every 30 meters while a vehicle is in motion, and every 30 seconds while at rest. Companies that declined to share location information of the scooters were only given a provisional permit that lasted 30 days.

Were we are speaking of a substantial business organization for a commercial purpose, such a practice would arguably contradict the CCPA. Section 1798.125 of the CCPA prohibits a business from discriminating against consumers for exercising certain rights under the law, including the requests to opt out of the sale of personal information (where sale is defined broadly as exchange of data for valuable consideration — here, a permit). The major goal of the nondiscrimination provision is to prevent companies from creating a "pay-for-privacy" situation.

In other words, companies may offer you privacy protection by default, but relinquishing such protections may offer you significant benefit. It could be argued that this potentially coercive aspect is even more amplified where the government is involved because the government does not operate in a free market — it ultimately holds the key to permit private parties to operate. Here, for example, it may be that the Los Angeles DOT’s policy regarding scooter permits would be discriminatory, as it does not permit a company to refuse to share a consumer’s data without taking away the benefit of a longer permit.

On the other hand, perhaps such collection and use of personal data is not discriminatory for two reasons: (1) it is purportedly not for a commercial benefit, and (2) the consumer’s choice in this instance is binary: they can use the product, or not. Specifically, one could argue that the government — including the Los Angeles DOT — has the responsibility to protect its citizens, including with respect to transportation regulations, and that such a noncommercial collection of data is not for a coercive or discriminatory purpose. Further, the Los Angeles DOT’s offer may be discriminatory toward the company at issue, in that the company can only get a longer-term permit for providing data, but the consumer is not treated differently based on his or her willingness to share personal data.

This dynamic, with the company as a middleman between the consumer and the government, also presents an interesting situation with respect to consumer requests. For example, the CCPA allows for a consumer to request deletion of his or her data (subject to exceptions). If the data is personal information, and a consumer asks to delete their data from the scooter company, would the scooter company be able to ask the Los Angeles DOT to delete this information from their records as well? What teeth would such a request have if the government is not also bound by the CCPA?

It could also be argued that this data is not “personal information” — and therefore exempted under Section 1798.140(o)(2) of the CCPA — because it does not relate to an individual. In theory, the location data shared with the Los Angeles DOT is "anonymized"; indeed, the Los Angeles DOT confirmed that the shared data does not include the name, age, gender or address of the scooter users. However, anonymity is an elusive concept, not equivalent to removing only the data fields containing personal identifiers.

As one New York Times article points out, individuals can be identified relatively easily from patterns of movement. In that article, supposedly "anonymous" data showed repeated patterns of someone leaving a house in upstate New York at 7 a.m. and traveling to a middle school 14 miles away, and returning late in the afternoon. This pattern could easily be traced to a specific individual who carried her smartphone with her. Similarly, in this case as well, what the Los Angeles DOT may consider "anonymous" data can perhaps be used to identify people and their habits.

And the question becomes even more interesting when the government decides to share that information with the public. While the Los Angeles DOT agrees to keep this scooter information confidential, various other cities are set to publish some of this data. For example, Austin, Texas and Washington, D.C., make summaries of this data publicly available online. If the government decides to publish this data, then the data itself will necessarily be exempted from the CCPA (as publicly available data), even if use by another party would be subject to the CCPA, so long as the downstream use is consistent with the purpose for which it was publicly maintained.[1]

And if A.B. 874 — a proposed amendment to the CCPA — is signed into law, then even the guardrail of a "consistent purpose" would be removed, allowing anyone to use the publicly available data. As a result, some may assert that any regulation would likely be best applied at the beginning of the data-sharing stream to the government, as there are no other contours to guide even the public sharing of that data. On the other hand, public disclosure of information by the government may in fact be required by certain laws, such as the various Freedom of Information Acts. Limitations on such disclosure may then be at odds with the benefits of liberal government information sharing.

With constantly changing ideas of what it means to be surveilled, it may be time to reconsider what, if any, limitations on the government's collection and use of personal information should and do exist. The potential loopholes above suggest that there may be no defensible rationale to exempt government entities from such privacy laws, and that in fact, government entities should not be treated differently from other businesses that deal with personal data, including with respect to collection, discriminatory practices and data sharing. While the Los Angeles DOT and other cities have detailed various aspects of their policies and information handling practices, assisting with transparency, without legal recourse — privacy laws applying to government agencies — citizens may remain at the mercy of the agencies to protect their privacy.

Mark Lyon is a partner and Cassandra Gaedt-Sheckter and Arjun Rangarajan are associates at Gibson Dunn & Crutcher LLP.

[1] (Section 1798(o)(2)).