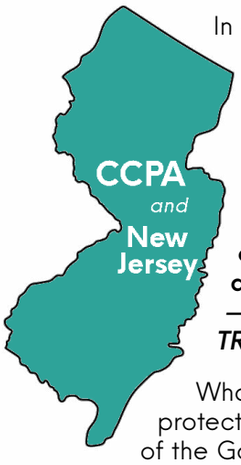
CCPA & NJ: How California's Privacy Law Affects Business in NJ

By Larry Samilow,
Co-Founder and Managing Partner
Verve Group Consulting

With the California Consumer Privacy Act, or CCPA, now in effect, businesses in New Jersey that are subject to the new law are scrambling to make sure that their public-facing privacy notices reflect the law's requirements and that their internal policies and procedures mesh with the specifications of this groundbreaking law, as well. Keeping employees up to date on fairly rapid changes in this area and making sure new training is developed and provided are keeping compliance professionals busy, too.

CCPA's Impact on NJ
The California law requires greater transparency so consumers are aware of why their personal information is being collected and used. The law also provides consumers with the ability to "opt out" of the transfer of their data to some third parties.



In certain circumstances, consumers in California can even have their private information deleted entirely. At the same time, the law is inspiring corporations to take greater precautions when handling personal information and to rethink their need for generating certain data in the first place. It's an interesting moment to try and make a business case for the collection and use of personal information. Justifying the need for and the sale of personal data, especially the more sensitive sort, just became a bit harder.

What's on your data privacy to-do list for 2020? "Balancing the Company's ability to use consumer data to help improve the services it offers against the need to comply with rules around such use."
— Laurie A. Poulos, Vice President, General Counsel, and Chief Compliance Officer, TRANZACT

What's even more interesting is that some corporations are extending some of the California law's protections to their entire U.S. customer base and not just limiting the CCPA's benefits to the residents of the Golden State. After all, the theory goes, some customers shouldn't be more equal than others. Why shouldn't a citizen of New Jersey receive the same benefits a citizen of California gets—especially from a business that happens to be based in the Garden State?

A Dazzling Array of Privacy Regulation with More on the Way
Adding to the challenge is the fact that before New Jersey corporations try to do the right thing with regard to data privacy, they are facing the reality that more than one law applies to their efforts.

• For example, some lucky organizations have to navigate the European Union's General Data Protection Regulation, or GDPR, which went into effect in 2018. That law, which in many ways is more extensive than California's, focuses in some measure on an organization's legal basis for processing personal information.

• Complicating well-intended compliance even further is the recent Brexit saga. How exactly the UK's withdrawal from the European Union will impact data protection in the long term is still not entirely known.

At the federal level in the United States, some laws already touch on data privacy, such as the Health Insurance Portability and Accountability Act, or HIPAA, which safeguards health information. The Children's Online Privacy Protection Act, or COPPA, pertains to the protection of personal information collected online from minors, and elements of the Gramm-Leach-Bliley Act are geared toward the protection of consumer financial information. A number of data privacy bills have been introduced in Congress.

> **"As a company that does business nationwide, it is challenging to contend with the patchwork of varying, potentially conflicting and often unclear, state and federal privacy laws and regulations. The strong preference is to have a clear, federal privacy law that preempts all state privacy laws."**
> ***— Laurie A. Poulos, Vice President, General Counsel, and Chief Compliance Officer, TRANZACT***

Closer-to-home requirements apply to New Jersey enterprises, as well. Companies must already disclose breaches of the personal information of residents of New Jersey under the Garden State's breach notification law. Further, a number of bills introduced in the New Jersey legislature address data privacy in one form or another.

In the end, greater data privacy regulation likely is in all of our futures.

Why Does All of This Matter?
Good privacy hygiene does, of course, help companies avoid enforcement actions, fines, lawsuits, professional embarrassment and harm to reputation. But even if some subpar privacy practices somehow have eluded the media's glare, they likely will come to the surface during any due diligence effort in, say, a merger or acquisition.

> **Some "privacy concerns during M&A due diligence" can be alleviated "from the infancy stages" of a project, suggests Greg Berkin, Vice President, IT & Cybersecurity, and Chief Information Officer at Caladrius Biosciences, Inc. One hazard is allowing "data to get into the wrong hands."**

With a fairly healthy M&A market forecast for the year ahead, no one wants to lose out or lose ground on a money-making deal because of lackluster privacy practices. Buyers do not want to acquire a legacy privacy problem. To that end, it is vital for IT, legal, compliance and business teams to work collaboratively to address privacy concerns.