#ForensicPerspectives

CCPA and e-discovery

Go with the CCPA flow

There is a range of commentary on the development of the CCPA and its continuing transformation by the California legislature. Rulemaking uncertainty combined with extensive lobbying power could complicate e-discovery if there is confused and inconsistent enforcement, as well as challenges to specific provisions or the entire law.

Protect personal information by policy

The CCPA has a broad definition of personal information, which can complicate the collection, processing, review, and production of electronic discovery. Any information that can reasonably identify or be associated with an individual or a household requires protection. Since this can range from common contact details to biometrics, location coordinates, and online search history captured in potentially unstructured databases, parties may want to update their agreements to ensure compliance with all relevant CCPA obligations in litigation.

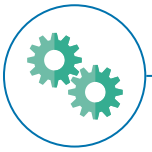
Respect the right to delete

With a few exceptions, such as to protect against malfeasance, properly engage in business with the consumer, or for legal requirements, the CCPA gives individuals the right to request that companies permanently delete their personal information. The challenge is for organizations to balance the retention of consumer data for legal hold and other potentially valid litigation-related purposes and updating their methodology for storing, processing, and potentially erasing personal information to comply with the CCPA.

Beware of the right of action

Disclosure of certain consumer information, such as names combined with social security numbers, driver's license details, and bank account records, among other data points that are not publicly available, including erroneously sharing them in litigation or failing to use reasonable security procedures gives consumers a right of action and the potential for statutory damages under the CCPA. Since those provisions could prompt an array of lawsuits, proper e-discovery practices are critical for ensuring compliance with the new provisions.

CRA Charles River Associates



Develop systems for data subject access requests

When California residents request their personal information under the CCPA, that Data Subject Access Request (DSAR) will require identity verification, a full records search, data collection, evaluation and potential modification of the results, and production within 45 days. For large organizations, technology is the only option for managing what is likely to be a significant number of applications, which every California resident can make twice per year. Given the similarity of this process to a typical demand for information in litigation, adapting e-discovery tools to automate and process these requests will become essential.

Understand privacy laws beyond the CCPA

While the CCPA specifically provides for deference to federal laws governing protected health information under the Health Insurance Portability and Accountability Act, and credit data under the Gramm-Leach-Bliley Act, it does not conclusively address potential conflicts with existing state provisions focused on privacy safeguards, such as breach response rules and privacy policy designations. As a result, the potential for confusion could have a material impact on discovery and litigation support.

Recognize that Employees are not consumers under the CCPA…yet

The CCPA excludes the personal information of employees, job applicants, contract workers, and agents from the law for one year, regardless of whether they are California residents, who are otherwise subject to its provisions. As a result, a company that collects information for employment or similar purposes would be excluded from compliance. When managing e-discovery requests and processes, this distinction could be critical since it could eliminate entire HR or other systems from scrutiny until January 1, 2021.

Avoid penalties for non-compliance

CCPA enforcement will continue to evolve and complicate e-discovery. CRA's Forensic Services team offers expert guidance in these matters. Our experts combine expertise in forensic accounting, computer forensics, technology, valuation, and business intelligence. To continue the conversation, please contact one of the experts listed below.

Kristofer Swanson, CPA/CFF, CFE, CAMS
Vice President & Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com

Josh Hass, CFE, CEDS
Vice President, Forensic Services
+1-212-520-7139 | jhass@crai.com