COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2020
The CCPA and when privacy law overlooks internal compliance functions

By Stuart L. Pardau

Stuart L. Pardau (stuart.pardau@csun.edu) is a tenured professor at the David Nazarian College of Business and Economics at California State University, Northridge, USA. He also practices law and consults with clients in the areas of privacy and data security, intellectual property licensing, and compliance issues.

Experience informs us that it is not uncommon for different areas of law to conflict and sometimes produce unintended results. The intersection of privacy law and corporate compliance produces some disturbing examples in this regard.

As Exhibit A, take the Federal Trade Commission's 1999 ruling that the Fair Credit Reporting Act (FCRA) required employers to obtain an alleged sexual harasser's consent before having the employer's outside law firm investigate the allegations, or Article 10 of the General Data Protection Regulation (GDPR), which limits the "[p]rocessing of personal data relating to criminal convictions" without carving out exceptions for internal investigations, anticorruption due diligence, export control vetting, or background checks on potential employees.[1]

Similarly, the GDPR's right to be forgotten, right to object to processing, and right to restrict processing can hamstring internal investigations and due diligence related to hiring. In these and other cases, well-meaning privacy advocates and well-intentioned drafters of statutes fail to unambiguously allow processing of personal data for legitimate compliance and ethics purposes.

The CCPA's problematic definitions

The California Consumer Privacy Act[2] (CCPA) is yet another example of a law that fails to properly countenance compliance issues. Effective January 1, 2020, CCPA provided California "consumers" (defined as residents of California) with a bundle of new privacy rights, including the right to opt out of the sale of personal information, the right to request deletion of personal information, the right to access personal information, and the right to know what personal information a business has collected and how it is sharing and using that personal information.

Because the definition of consumers does not exclude employees, CCPA applies to all employees who are residents of California, and all references to consumers under the law can be read as references to California employees as well. While CCPA has partially delayed applicability to human resources/personnel information until January 1, 2021 (there is only a limited notice requirement in 2020), all of the above rights will apply to employees after that date. After January 1, 2021, will a California employee have the right to request that his or her employer delete personal information related to potential wrongdoing? If an internal investigation is ongoing, does the employee have a right to know any information the business is collecting from other sources in connection with that investigation?

CCPA and compliance issues

While there are some helpful exceptions to these new rights, it is far from clear that they are sufficient safeguards for compliance efforts. For example, Section 1798.110 provides an exception to the deletion right "[t]o enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" or where the employer would "[o]therwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."

But what constitutes a "lawful manner" of use, and when is that use "compatible with the context" in which the information is provided? Moreover, each of these exceptions is premised on the information remaining internal. Does this preclude the involvement of outside organizations, like law firms, who are routinely involved in internal investigations? Does this also preclude voluntary disclosures of the results of an internal investigation to law enforcement authorities?

Furthermore, the above exceptions only apply to an employee's deletion right and would be of no use in a scenario where an employee asserted a right to know or even to access the contents of an internal investigation.

Although there are other exceptions that apply generally to the law, and not just to the deletion right, they are not sufficient to protect legitimate compliance and ethics interests. Nor will they prevent a culpable employee from making claims under the law to slow an investigation or cause a company to settle rather than fully complete its efforts. Section 1798.145 states that the CCPA shall not restrict a business's ability to:

> 1. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
> 2. Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
> 3. Exercise or defend legal claims.

But often, compliance issues arise before any civil, criminal, or regulatory proceedings are formally initiated, before law enforcement agencies are involved, and sometimes even before a business is aware of a potential legal claim. As the regulations are currently written, none of the exceptions discussed above would protect a company from situations where an employee is aware of wrongdoing, and requests that an unwitting business delete information that could later be used as evidence against the employee, thereby subverting the investigation process before it has even started.

In addition, businesses will face real choices about whether to comply with CCPA or risk running afoul of federal laws requiring robust compliance programs, triggering Supremacy Clause questions that, ultimately, courts will have to clarify. Likewise, a company deleting adverse personal information at the request of an employee may risk a charge of spoliation of evidence under certain conditions.

Find the balance

To be prepared for these choices, compliance and ethics professionals should familiarize themselves with CCPA, GDPR, and other key privacy laws to identify potential conflicts. With the help of legal counsel, they should also develop protocols for dealing with employee privacy requests in a way that does not conflict with compliance interests and should consider other mitigation efforts to deal with the negative impact of privacy laws. These mitigation efforts should include, at a minimum, disclosures in employee handbooks regarding potential use of personal information for compliance and ethics uses (to bolster the argument that such uses are "reasonably

aligned with the expectations of the consumer"), procedures to ensure information is not deleted before first ascertaining whether it may be retained pursuant to a lawful exception, and thorough documentation procedures to demonstrate compliance.

Conclusion

These issues are serious and have likely not been considered adequately, if at all, by CCPA drafters and regulators. While there is not necessarily any right way to close these loopholes, the best way would be to enact legislation that recognizes the importance of corporate compliance and ethics programs and that provides broad protection for compliance work.

Alternatively, the California legislature (and others with similar laws on the books) should amend existing privacy laws to adequately account for compliance and ethics programs. Whatever the solution, the CCPA, like other privacy laws, including GDPR, is in dire need of adjustment. Otherwise, valid compliance and ethics objectives will be unintentionally compromised in the name of privacy, and the ability to prevent and detect serious wrongdoing will be undermined.

Acknowledgments

The author would like to thank Joseph Murphy for his extensive comments, feedback, and edits to various versions of the draft.

Takeaways

- Future laws and regulations need to better align with the requirements of internal compliance and ethics programs.
- The California Consumer Privacy Act (CCPA), as the model for other privacy laws in the country, should be modified to address important compliance and ethics interests.
- Compliance and ethics professionals should familiarize themselves with the CCPA, the General Data Protection Regulation, and other privacy laws to identify potential conflicts.
- Compliance and ethics professionals should develop protocols for dealing with employee privacy requests in a way that does not conflict with compliance interests.
- Compliance and ethics professionals should consider other mitigation efforts to deal with potential negative impacts of privacy laws.

1 TRACE International, *Public Comments: Review of the 2009 Anti-Bribery Recommendation,* OECD Working Group on Bribery, accessed June 2, 2020, 81-89, https://bit.ly/2Mnuuuu.
2 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 to 1798.198 (West 2018).