US Law Week
Nov. 5, 2024, 4:30 AM EST

California's Costly Privacy Update Raises Free Speech Questions

- *Squire Patton Boggs attorneys examine plan set for Nov. 8 vote*
- *Would cost billions of dollars, push First Amendment boundary*

With the burden of data privacy compliance appearing to increase unabated in the US, it's time to reflect on whether the benefits from all this regulation have been and will be worth the considerable financial and free speech burdens they place on businesses.

US regulators need to be mindful that the EU lacks the editorial and commercial speech protection that the US Constitution provides commercial enterprises, so importing the EU's General Data Protection Regulation concepts without sufficiently Americanizing them will run afoul of the First Amendment.

The need for this reflection is growing more apparent with recent actions in California, where the state's privacy protection agency's board plans to vote whether to advance proposed regulations to public comments on Nov. 8 that address cybersecurity audits; automated decision-making technology, including artificial intelligence, profiling, and privacy risk assessments; and other updates to existing regulations.

The agency recently published an impact assessment estimating that the regulatory impacts of the proposed regulations would exceed $4 billion in the first year of implementation. It is worth noting that the impact—a conservative estimate—is 80 times the $50 million threshold for what California considers to be a "major regulation."

The estimates don't include the compliance costs incurred by businesses that aren't based in California but must comply with the state's privacy law because they do business in California. Considering that government estimates of economic burden often are far less than what is realized, the burden created by the proposed regulations will likely exceed even the staggering $4 billion estimate.

For instance, the agency estimated that the costs of complying with this rulemaking should be calculated based on the initial cost of developing compliance software systems of $21,874 to $32,810 per business and that ongoing annual operational costs would be 15% to 30% of that. Based on our experience with clients, that is an exceptionally low estimate and far from inclusive of all applicable costs, such as legal counsel and compliance personnel.

The impact assessment estimated that this would lead to a $3.5 billion direct cost to businesses that are subject to the state's privacy law, creating a larger adverse impact because it would directly affect cost and profit margins. The investment shortfall could reduce current output by $50 billion, employment by 98,000 full-time positions, and gross state product of $27 billion.

To those worrying that the cost for these proposed regulations would be an unjustified burden on companies doing business in California, the agency posits that the benefits of stronger consumer privacy protection "far outweigh these costs in the long run, improving the investment climate and overcoming cumulative adjustment costs incurred by California businesses."

The impact assessment failed to address considerations of burdens related to but extending beyond the cost, such as free speech.

In *Sorrell v. IMS Health*, the US Supreme Court held that "the creation and dissemination of information" is a free speech right. Even if considered commercial speech and intermediate scrutiny applied, the restrictions must both directly advance and substantial state interest in a way that a more limited restriction couldn't accomplish.

Mandating the publication of assessments that call for making value judgments has been found to be compelled speech, subject to at least intermediate and potentially strict scrutiny. In *Netchoice v. Bonta*, the US Court of Appeals for the Ninth Circuit struck down the data privacy impact assessment and content transparency requirements as unconstitutionally burdensome, noting that state data privacy impact assessment requirements, if properly tailored, may "not necessarily" be similarly unconstitutional.

In another case, the D.C. Circuit examined the difference between requiring merely factual disclosures in paid advertising, which courts scrutinize with deference to regulators, and requirements that public companies disclose in public filings with the Securities and Exchange Commission their use of "conflict minerals" — those obtained from the war zone in the Democratic Republic of Congo—to which it applied intermediate scrutiny. It found that such a reporting requirement was unconstitutional.

So, to pass constitutional muster, California's proposed regulations need to advance the state's interest in protecting consumers in a way that doesn't ignore materially less burdensome alternatives that would achieve the same result.

Other states with data privacy impact assessment requirements omit details on how companies should assess their practices and corresponding costs, risks, and benefits. Those states allow businesses to determine how they should evaluate their statutory duties of transparency, choice and control, governance and diligence, purpose limitation and data minimization, risk mitigation, reasonable security, and accountability.

However, Colorado prescribes consideration of up to 35 specific issues and requires documentation of acceptable risk conclusions. California's privacy law calls for even more to be considered and documented. Note that this is before California has even proposed requirements for cybersecurity audits.

California and Colorado could achieve their consumer protection goals by merely suggesting best practices for how companies could assess their activities, considering their data privacy and security safety obligations, without creating a specific and burdensome administrative process or publishing conclusions as to what is acceptable and unacceptable benefits or harms to consumers.

Much of what Colorado and California seek to mandate can be seen as good information governance hygiene. However, requiring specific questions and considerations, and mandating that results and conclusions be published and made available for inspection, is simply a bridge too far.

This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Alan Friel is chair of Squire Patton Boggs' data privacy, cybersecurity, and digital assets practice.

Glenn Brown is principal and a senior member of Squire Patton Boggs' data privacy, cybersecurity, and digital assets practice.

Write for Us: Author Guidelines

To contact the editors responsible for this story: Rebecca Baker at rbaker@bloombergindustry.com; Daniel Xu at dxu@bloombergindustry.com