NELSON HARDIMAN
HEALTHCARE LAWYERS

Privacy Watch: CPRA Enforcement Delayed Until March 2024

Regulatory Update

Privacy Watch: CPRA Enforcement Delayed Until March 2024

The explosive growth in corporate reliance on cloud systems for operations and the pervasive use of social media for marketing have inadvertently created numerous channels for potential transmission of sensitive personal data. Although hacking and unintentional security lapses have led to significant data leaks, the bulk of information sharing is deliberate. A recent Senate report pointedly accused prominent tax filing services like H&R Block, TaxAct, and TaxSlayer of "recklessly sharing tens of millions of taxpayers' personal and financial data" with tech behemoths like Facebook and Google. Investigations into the realm of sensitive medical data revealed similar practices, with hospitals sharing patient information with social media firms. Beyond the scope of advertising, data sharing has become a routine practice in healthcare, spurred by federal laws like HIPAA and HITECH which ignited the seismic shift to electronic record keeping. It wasn't until recently that the FTC stepped onto the stage as a 'healthcare privacy enforcement agency,' leaving the substantial burden of addressing these vulnerabilities predominantly on the shoulders of state-level legislations and law enforcement agencies.

The enactment of the California Consumer Privacy Act (CCPA) in 2018 marked an important step in enhancing privacy rights and protections for California residents. The CCPA introduced a series of new data privacy rights, ranging from the right to know what personal information a business collects, to the right to opt-out of the sale of personal information. In a continuation of this effort, voters passed the California Privacy Rights Act (CPRA) in November 2020. This proposition expanded upon the foundations laid by the CCPA, introducing additional consumer rights, stricter business obligations, and mandating the creation of a new enforcement body, the California Privacy Protection Agency (CPPA).

However, turning these extensive statutes into practical, actionable regulations for businesses has proven to be a complex, multi-year challenge for state officials. The agency only published a set of finalized rules on March 29, 2023 . Despite this, the CPPA remained committed to commencing enforcement of the new rules on July 1, 2023. This timeline was contested by the California Chamber of Commerce, which argued in court that it was too short for many companies to adhere to the new standards and requested a delay. The Superior Court agreed with this viewpoint, ruling that the enforcement of new regulations should not begin until **March 29, 2024.** However, the presiding judge maintained the validity of the laws themselves, ensuring their continued effect in the interim. For companies that have been slow to adapt, this grace period presents an invaluable opportunity to revisit public-facing privacy disclosures and refine their internal procedures for storage and sharing of sensitive personal information so they are compliant with latest rules.

Impact of Agency Enforcement on Digital Privacy

The implementation of these new privacy rules is intended to have a broad impact on businesses and consumers in California, particularly as they aim to address some of the more glaring vulnerabilities in data privacy involving sensitive personal data and how it is shared with third-party contractors. Some notable additions and enhancements enforced by the CPPA will include:

New Category of Sensitive Personal Information: The CPRA expands the concept of 'Sensitive personal information' which includes information that reveals a consumer's social security, driver's license or passport number, precise geolocation, racial or ethnic origin, certain types of financial account and login information, contents of certain messages, and genetic data. Consumers can limit the use and disclosure of such information. Cal. Civ. Code § 1798.140(ae)

Data Minimization and Purpose Limitation: The CPRA clearly mandates businesses to restrict data collection to what is necessary to accomplish the intended purpose of the original collection. Cal. Civ. Code § 1798.100(c)

Right to Request a Correction: The CPRA gives consumers the right to request that businesses correct inaccurate personal information. A business that receives a "verifiable consumer request" is obliged to use commercially reasonable efforts to correct the inaccuracy. Cal. Civ. Code § 1798.106

Automated Decision Making and Profiling: The CPRA includes provisions about profiling and automated decision-making, requiring businesses to provide meaningful information about the logic involved and the likely impact. Cal. Civ. Code § 1798.185(a)(16)

Extended Opt-Out Rights: Consumers can direct businesses to not only stop selling their information, but also stop sharing it with third parties. Cal. Civ. Code § 1798.120

Increased Penalties for Violations Involving Children's Information: The CPRA triples maximum penalties for violations concerning consumers under the age of 16. Cal. Civ. Code § 1798.155(b)

Contractual Obligations with Third Parties: The CPRA imposes direct obligations on businesses to enter into certain contractual provisions with third parties, service providers, and contractors to whom personal information is disclosed. Cal. Civ. Code § 1798.100(d)

It is clear that we are entering a new phase in privacy regulation, but it is worth noting that the CPRA's emphasis on consumer disclosures and notifications carries both promise and uncertainty. On one hand, these provisions equip consumers with unprecedented control over their personal data, addressing long-standing concerns about privacy and transparency. On the other hand, their effectiveness hinges on consumer action, raising pertinent questions about their real-world impact. Will consumers, for instance, capitalize on the opportunity to exercise their opt-out rights, and will they proactively request businesses to rectify their personal information? Equally important is the question of business compliance. Will companies embrace these changes wholeheartedly or try to preserve the status-quo, relying on opaque 'click-through agreements' or the prevalent consumer behavior of glossing over terms and conditions. The answers to these questions are set to shape the future of digital privacy. However, the prevailing consumer nonchalance towards online privacy agreements suggests an increasingly aggressive role for bodies like the FTC and CPPA in privacy enforcement will be necessary to effectively secure our digital futures.

Authors:

Tara Davidoff, Attorney, Nelson Hardiman

Yehuda Hausman, Law Clerk, Nelson Hardiman

Nelson Hardiman LLP

Healthcare Law for Tomorrow

Nelson Hardiman regularly advises clients on new healthcare law and compliance. We offer legal services to businesses at every point in the commercial stream of medicine, healthcare, and the life sciences. For more information, please contact www.nelsonhardiman.com