What businesses should know about data protection and enforcement in 2023

By Anna Mercado Clark and Paula P. Plaza
Phillips Lytle LLP

The new year heralds data protection laws, regulations and enforcement activity. For instance, various comprehensive (e.g., laws in California, Colorado, Virginia, Connecticut and Utah, which may also apply to businesses outside of these states) and targeted (e.g., New York City employment screening) privacy laws take effect in 2023. Meanwhile, regulatory bodies such as the Federal Trade Commission (FTC), which regulates most nonprofit organizations, are increasingly focused on enforcement. This article focuses on the California Privacy Rights Act (CPRA), New York City's employment screening law and FTC's consumer surveillance rulemaking.

Anna Mercado Clark
Partner

Paula P. Plaza
Associate (Admission Pending)

CPRA amends already comprehensive consumer privacy law

The CPRA, which took effect on January 1, 2023, amends the far-reaching California Consumer Privacy Act (CCPA). It modifies, among other things, the criteria that triggers the law, individuals' data rights, and the obligations imposed on covered businesses. For instance, whereas the CCPA applied to businesses that met various thresholds, including buying, receiving, selling or sharing personal information of 50,000 or more California consumers, households or devices, that threshold has now increased to 100,000 consumers and households, but devices were eliminated. The law grants consumers the right to correct inaccurate personal information, restrict the processing of sensitive personal information (a new data category), and opt out of sharing their personal information for cross-context advertising.

Failing to comply can carry penalties of up to $750 per consumer per incident or actual damages, and in certain circumstances, consumers may bring private causes of action to recover damages.

New York City's automated employment decision tool law

New York City employers that use automated decision tools (including artificial intelligence) in their hiring and promotion processes will be required to complete a bias audit by an independent auditor of such tools no more than a year prior to such use and provide certain prior notice to applicants or employees residing in New York City regarding their use. Failure to comply carries penalties ranging from $500 for the first violation and any additional violations on that day, and $500 to $1,500 per subsequent violation, where each day of non-compliant tool use shall constitute a separate violation. Failure to provide any notice shall be a separate violation. This law is presently scheduled to take effect on April 15, 2023.

FTC eyes regulation of commercial surveillance and data protection enforcement

The FTC recently sought public input on whether it should create new rules to address commercial surveillance and data protection practices. According to the FTC, commercial surveillance is the business of collecting, analyzing and profiting from consumer personal information. This information may be used to maximize advertisement effectiveness, such as by selecting the most advantageous time to release ads, identifying the most likely audience for their products or services, or customizing brand messaging (such as by reviewing browsing history and past purchases). The FTC is concerned, however, that these practices may increase the risk of consumer deception, discrimination and data breaches, among other things. Upon review of the public comments received, the FTC is expected to schedule a hearing, issue a recommended decision and, as appropriate, issue the rule.

The foregoing are just some developments on the horizon. Businesses are advised to track the latest developments in laws, regulations and enforcement activity and work with professionals who have the technical and legal expertise to guide them through the changing compliance landscape while considering their business needs.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400 ext. 6466.

Paula P. Plaza is an associate (admission pending) at Phillips Lytle LLP and member of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at pplaza@phillipslytle.com or (716) 847-8324.