Published on *The National Law Review* https://natlawreview.com

Privacy Report: California Privacy Protection Agency Releases Draft CPRA Regulations

Article By:

Eva J. Pulliam

Christine Chong

Destiny Planter

Headlines that Matter for Privacy and Data Security.

US News

California Privacy Protection Agency Releases Draft CPRA Regulations

The California Privacy Protection Agency (CPPA) just released proposed California Privacy Rights Act (CPRA) regulations. The regulations expand consumer protection as they provide more context about the right to correct inaccurate personal information and further explain the right to limit the use of sensitive personal information. Moreover, the regulations introduce a new alternative opt-out link, making it easy for consumers to exercise the right to correct inaccurate personal information and limit the use of sensitive personal information simultaneously. The regulations also feature more detailed consent requirements that businesses must follow to prevent dark patterns. The CPPA is required to adopt these regulations by July 1, 2022.

FTC's Full Bench of Commissioners Issue a Policy Statement on Education Technology and the Children's Online Privacy Protection Act

With the addition of Alvaro Bedoya, the Federal Trade Commission (FTC) now has a full commissioner bench. Just three days after Bedoya's swearing in, the commissioners unanimously took action by adopting a Policy Statement on Education Technology and the Children's Online Privacy Protection Act (Policy Statement). With the increased use of education technology (ed-tech) devices in the classroom and the ever-growing technologies that monetize personal information collection, the Policy Statement is extremely timely. It focuses on a few areas: (1) limitations on the use of personal information collected from children under 13 with the school's authorization for any commercial purpose, including marketing or advertising; (2) retention limitations, including that personal information should not be kept for longer than is necessary to fulfill the purpose for which it was collected; and (3) security requirements. The Policy Statement serves as a warning and

reminder that children should not have to surrender their privacy rights to learn. For more information, please see our alert here.

NAI Releases Report to Help Companies Avoid Dark Patterns

The National Advertising Initiative (NAI) published a report entitled Best Practices for User Choice and Transparency, which educates companies about dark patterns—also called "deceptive patterns" or "manipulative designs"—and how to avoid them. The report helps companies maximize notice and choice mechanisms. Additionally, the NAI uses the report to explain consumer choice and transparency obligations under the NAI Code of Conduct. Further, the NAI encourages businesses to incorporate the following practices: (1) complete disclosure; (2) accurate representation of data collection, use, and sharing; and (3) easy cancellation features. For notice statements, the NAI encourages businesses to be as concise as possible while including all material information. For choice options, the NAI encourages companies to avoid using "take-it-or-leave-it" options and "trick language." Finally, the report advises businesses to implement easy and seamless methods for users to cancel services.

DOJ and EEOC Warn Employers That Artificial Intelligence Technology Can Unfairly Discriminate Against People with Disabilities

The Department of Justice (DOJ) and the Equal Employment Opportunity Commission (EEOC) released technical assistance documents warning employers about the dangerous impacts artificial intelligence technology can have on employees with disabilities. While artificial intelligence is useful in helping employers screen applicants, select new employees, monitor performance, and determine pay raises, these same tools may result in unlawful discrimination against people with disabilities in violation of the Americans with Disabilities Act. Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring, the DOJ's guidance document, clarifies that employers must consider how their technological tools could impact people with disabilities and provides information for employees who believe they have experienced discrimination. The EEOC's document, The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees, discusses issues that employers should consider to ensure certain workers are not disadvantaged. Further, the EEOC's document focuses on the importance of employers having reasonable accommodations when using artificial intelligence.

President Biden Enacts Better Cybercrime Metrics Act

President Biden recently signed Senate Bill ('SB') 2629, also known as the Better Cybercrime Metrics Act, into law. The Act creates new requirements to improve the collection of data related to cybercrime and further encourages the protection of individuals' personal information. Under the Act, the Department of Justice (DOJ) must enter into an agreement with the National Academy of Sciences to develop a taxonomy for categorizing different types of cybercrime not later than 90 days after the Act goes into effect; the DOJ must establish a category in the National Incident-Based Reporting System for collecting cybercrime reports; and the Government Accountability Office must assess the effectiveness of reporting mechanisms.

Google Expands Privacy Controls and Announces New Security Features

Google recently announced new privacy measures that will allow users more control over their data and overall user experience. Under the My Ad Center interface, users can now customize and limit the types of ads they see. Additionally, users can now request that their personal information be

removed from search results. Further, Google plans to now use a strategy called “protected computing,” a transformed data processing approach where more data will be processed on devices as opposed to on Google’s cloud servers. The new features represent Google’s continued efforts to protect the privacy and keep the trust of its users. Please find
Google’s announcements here and here.

Privacy Shield 2.0 Still Not Up to Par According to Privacy Activist Max Schrems

Privacy activist and lawyer Max Schrems (Schrems) recently warned European Union (EU) and United States (US) policymakers that Privacy Shield 2.0, the most recent data transfer mechanism, is likely to have the same destiny as the original Privacy Shield and Safe Harbor Framework. Following the 2020 Schrems II decision invalidating the Privacy Shield due to concerns with government surveillance, EU and US regulators worked to develop a compliant framework. Earlier this year, the White House announced an agreement in principle to establish a Privacy Shield 2.0. While adopting several portions of the original Privacy Shield, the new version was set to incorporate additional measures to limit intelligence collection to areas where necessary and install additional oversight for US intelligence agencies to protect privacy and civil liberties, amongst other things. Now, in a letter to key officials, Schrems expressed that the improvements are still not good enough. According to Schrems, US and EU policymakers have failed to sufficiently address government surveillance and consumer redress concerns. Further, he warned that although he is hopeful that the final text will address the current shortcomings, his group is prepared to challenge the new framework if it falls short.

Global News

EDPB Releases Guidelines on Law Enforcement Officials Using Facial Recognition Technology

The European Data Protection Board (EDPB) has released Guidelines on the Use of Facial Recognition Technology in the Area of Law Enforcement. The guidelines address lawmakers and law enforcement authorities who use facial recognition technology (FRT) systems, noting that FRT directly impacts fundamental rights and freedoms. Additionally, the guidelines advocate banning FRT in cases where it is used to infer a person’s emotions and in cases where it is used with personal data collected via scraping. The guidelines encourage officials to document the chosen FRT system, create user manuals, explain the technology, train end users on how to use the technology, and consult the appropriate data protection supervisory authority if necessary. After deploying the FRT, the EDPB encourages said officials to incorporate human oversight, a risk assessment process, and a protocol for data breaches.

OPC Says Context Matters in Deciding What Information is Sensitive

The Office of the Privacy Commissioner of Canada (OPC) recently issued an Interpretation Bulletin providing more context on what is considered sensitive information. According to the OPC, context is relevant to the assessment of sensitivity when deciding what personal information is sensitive and what information is not. Under Clause 4.3.4, any information can be sensitive, depending on the context. For example, email addresses can be considered sensitive information in certain contexts. Moreover, information that might be innocuous in one context can be considered sensitive when compounded with other information that may reveal an individual’s personal activities and preferences. The OPC also provides an overview of information that has been regarded as sensitive in the past, such as personal information affecting an individual’s reputation; financial information;

health information; drug and alcohol use; references to loneliness and depression; information that reveals sexual practices, preferences and fantasies; and political affiliations.

France's CNIL Publishes Guide for AI Systems

The French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertes (CNIL), recently published a GDPR compliance guide for artificial intelligence systems. The content is aimed at the general public, data controllers and processors, and artificial intelligence specialists. In the guide, the CNIL mentions the main principles of the Data Processing Act (Act No. 78-17 of 6 January 1978) and encourages data processors and controllers to follow these principles while using artificial intelligence systems to process data. The press release is here, and the guide is here, both only available in French.

Britain's ICO Fines Clearview AI £7.5M for Biometric Data Breach

Britain's Information Commissioner's Office (ICO) has ordered Clearview AI, a facial recognition platform used by law enforcement, companies, universities, and individuals, to pay £7.5M for breaching data protection laws in the United Kingdom (UK). According to ICO, the facial recognition software company illegally collected social media images of individuals without their knowledge. Further, the ICO claims that Clearview AI's actions of collecting images of people all over the world and creating a database that "not only enables identification of those people, but effectively monitors their behavior" are unacceptable and forces the watchdog to act to protect people in the UK. The chief executive of Clearview denies these allegations, claiming the company only collects public data from the internet. Please find the monetary penalty notice here. Please find the enforcement notice here.

NCSA and C4IR Launch a Data Protection Office in Rwanda

The National Cyber Security Authority (NCSA) and The Centre for the Fourth Industrial Revolution Rwanda (C4IR), an organization that uses government, industry, and academia to design, test, and refine policy frameworks, recently launched a data protection office in Rwanda. The data protection office will spearhead activities that ensure the protection of personal data and guarantee the privacy of individuals. Further, the data protection office will strengthen the privacy focus in Rwanda by overseeing data controller and processor registrations, compliance audits, data processing, computer technology research, and complaints. Find the press release here.

Singapore's Data Protection Commission Issues Biometric Data Guidance

After observing more incidents involving the mishandling of biometric data, the Personal Data Protection Commission (PDPC) published a Guide on the Responsible Use of Biometric Data in Security Applications for building owners, security service companies, and employers. The guide features key terminology; best practices to collect, use, and disclose biometric data responsibly; and an overview of how the Personal Data Protection Act's obligations apply to biometric data. It also features a practical guide for deploying security cameras that encourages placing notices at prominent locations to notify individuals that security cameras are in operation. Further, it features a practical guide for deploying access control systems to buildings or applications that encourages accuracy, database protection, and staff and vendor training. The guide also includes a sample template for adaptation by organizations for surveillance.

National Law Review, Volume XII, Number 159