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

Colorado Attorney General Seeks Rulemaking Comments for the Colorado Privacy Act

Article By:

Eva J. Pulliam

Christine Chong

Destiny Planter

US News

Colorado Attorney General Seeks Rulemaking Comments for the Colorado Privacy Act

With the Notice of Proposed Rulemaking set for fall 2022, Colorado's Attorney General office is currently inviting preliminary comments for the Colorado Privacy Act. Specifically, the office is interested in comments related to dark patterns, data brokers, and opt-out mechanisms. For those interested in submitting comments, the comment form is here.

Utah Publishes US's Latest Comprehensive State Privacy Law

Senate Bill 227, the Utah Consumer Privacy Act, was recently signed into law and will take effect December 31, 2023. The provisions include consumer rights, 45-day request response periods, a 30-day cure period, and attorney general enforcement provisions. See our updated Privacy Report with more information on the Utah Consumer Privacy Act here.

Artificial Intelligence: NIST Risk Management Framework and Guidance Addressing Bias in AI

The National Institute of Standards and Technology (NIST) recently released a draft of its AI Risk Management Framework (Framework) and Guidance to address bias in AI. The Framework addresses risks in the design, development, use, and evaluation of AI systems. The Guidance offers considerations for responsible development and use of AI. See our alert with a breakdown of the Framework and Guidance here.

Privacy Shield 2.0 On The Horizon

The European Union (EU) and the United States (US) recently reached an agreement in principle for a "Privacy Shield 2.0" that will replace the original Privacy Shield Framework that was invalidated in July 2020. Under Privacy Shield 2.0, the US is set to implement new safeguards to "ensure that

signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives." Companies transferring personal data from the European Economic Area (EEA) should be aware of Privacy Shield 2.0 as it may serve as an additional safeguard in growing privacy programs. See our client alert here.

Efforts to Combat Cyberattacks Ramp Up: President Biden Signs Cyber Incident Reporting for Critical Infrastructure Act into Law

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was signed into law on March 15, 2022. The Act aims to organize a national response to cyberattacks. CIRCIA has two main parts, one aimed at the federal Cybersecurity and Critical Infrastructure Agency (CISA) and one aimed at operators of critical infrastructure. First, CIRCIA increases funding for CISA, the agency that outlines "covered cyber incidents"—incidents that should be reported. According to CISA, covered cyber incidents include attacks that result in a monumental loss to an information system and result in destructive unauthorized access. Though there is a current framework of what a covered cyber incident entails, CISA has two years to issue further rules and definitions regarding cyberattacks. Second, CIRCIA requires operators in "critical infrastructure" sectors to report cyberattacks to CISA within 72 hours and ransom payments within 24 hours. Critical infrastructure sectors include Information Technology, Healthcare and Public Health, Government Facilities, Energy, Emergency Services, and other sectors "so vital to the United States that the incapacity of such systems would have a debilitating impact on the security of the United States." These entities are set to be further and more specifically defined by forthcoming rules.

Global News

CNIL Publishes Guidance on Processor Re-use of Personal Data

??The French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertes (CNIL), recently published guidelines for data processors that reuse personal data. The guidelines provide specific conditions where data processors can lawfully reuse personal data under the General Data Protection Regulation (GDPR). Reuse may be lawful under the following conditions: in situations (1) involving conclusive compatibility tests specific to the situation presented; (2) where prior and general authorization was prohibited; and (3) where the data controller has given authorization in writing. In addition, the guidelines state GDPR principles such as purpose limitation and lawfulness still apply. Lastly, the guidelines also make clear that while reusing personal data is permissible in the aforementioned scenarios, further processing is still prohibited under the GDPR. The guidelines are available here in French only.

EDPB Adopts Guidelines on GDPR Article 60, a Toolbox on Essential Data Protection Safeguards, and Guidelines on Dark Patterns in Social Media Platform Interfaces

The European Data Protection Board (EDPB) adopted Guidelines on Article 60 of the GDPR on March 14. The Guidelines provide an explanation of GDPR cooperation between supervisory authorities and aim to promote the one-stop-shop mechanism's legal provisions. Specifically, the one-stop-shop feature is a single contact point mechanism that allows companies doing business in more than one EU state to communicate with a lead Data Protection Authority (DPA) or Supervisory Authority (SA), as opposed to DPAs or SAs in each jurisdiction. In turn, Article 60 of the GDPR regulates the cooperation procedure between the lead SA and other SAs involved—the authorities who are also impacted by the effects of the processing activities. Under the Guidelines, SAs are able to merge their own national procedures with the one-stop-shop feature. The Guidelines endorse a

collaborative approach whereby the parties exchange relevant information and investigate cases together.

Second, the EDPB adopted a toolbox on essential data protection safeguards for enforcement cooperation between EEA and third country SAs. The toolbox features definitions, data processing principles, rights of data subjects, compliance with data protection principles, and can be used by SAs as well as the European Commission.

Third, the EDPB adopted Guidelines on dark patterns in social media platform interfaces for social media designers and users. The Guidelines offer practical recommendations to prevent users from falling victim to dark patterns and making unintended, potentially harmful decisions regarding the processing of their personal data. The Guidelines list examples of dark patterns such as: overloading: hounding users with a large quantity of requests; skipping: manipulating users so they don't pay close attention to the data they provide; stirring: appealing to users' emotions to impact the data they provide; and hindering: forcing users to provide data by making the site hard to navigate without it being provided. Moreover, the Guidelines encourage social media designers to implement the following best practices for GDPR compliance:

1. Include a Table of Contents in Privacy Policies to make them easier to navigate
2. Include the identity of the SA and a link to its complaint website
3. Clearly and precisely state the purpose of processing
4. Provide definitions of technical words or jargon

ICO Publishes Guidance on Lawful Use of Video Surveillance Systems

The Information Commissioner's Office (ICO) published guidance to help public and private organizations, including non-criminal law enforcement authorities, that use video surveillance systems. The Guidance emphasizes ensuring surveillance systems only capture surveillance in alignment with the specific purpose for which it is being used; identifying the minimum amount of personal data needed for processing purposes; and storing information securely. It covers surveillance systems such as dashcams, smart doorbell cameras, CCTV, Automatic Number Plate Recognition (ANPR), Body Worn Video (BWV), Facial Recognition Technology (FRT), and Drones (UAVs). The guidance does not apply to all surveillance systems. Specifically, it does not apply to individuals recording footage in a purely personal or household context.

China Passes Regulations Requiring Companies to Disclose Algorithms

China's new law with requirements on companies' use of algorithms recently went into effect. Under the new requirements, companies must provide conspicuous notice to users if algorithms are being used to promote content. Users must also be allowed to opt out of such algorithms. Separately, there are provisions addressing fake news which prohibit companies from generating and aggregating fake news. The set of regulations are available here in Chinese.

China's Regulatory State Agency Releases Second Draft of Measures for Data Security in Industry and Information Technology

The Ministry of Industry and Information Technology (MIIT) recently released its second draft of Interim Administrative Measures for Data Security in Industry and Information Technology (Draft Measures) in China. Although the MIIT published its first draft back in Fall 2021, the most recent draft features updates to adopt and address public comments received by MIIT after the first draft. The Draft Measures provide context to the Data Security Law, which aims to divide data into different levels based on its importance and associated harm. According to the measures, data falls into three categories: ordinary data, important data, and core data. While ordinary data is data that has a relatively low impact on public interest in the event of a breach, core data is data posing a serious threat to the security of politics, territories, militaries, etc. Further, the Draft Measures pose general security obligations for processors, including hosting data security training and drafting contingency plans in the event of a breach. Updates are expected to come by September 2022.

Chile's Consumer Rights Protection Agency Rolls Out New Artificial Intelligence Personal Data Processing Guidelines

El Servicio Nacional del Consumidor (SERNAC), Chile's consumer rights protection agency, recently rolled out mandatory Artificial Intelligence (AI) data protection rules. According to the rules, AI controllers must remain in compliance with data protection rules during every stage of processing. Additionally, these controllers must obtain a valid legal basis for processing, provide data rights such as access, deletion, and opposition, and maintain transparency about the processing.

Norwegian Regulator Releases New Guidance on Employee Background Checks

Datatilsynet, the Norwegian data protection authority, recently published a Guide laying out when employers can run different types of background checks. According to the Guide, background checks that feature police certifications can only be required when the law or regulations allow them. Moreover, integrity investigations—investigations that collect information on corruption, crime, and special categories of personal data—can only be carried out with prior approval from Datatilsynet. Finally, credit ratings are only permissible in instances where an employee's credit is necessary to the interests of the work. The Guide is available in Norwegian here.

National Law Review, Volume XII, Number 98