HINSHAW

Alerts

# Hindsight is 2020: Data Privacy Law Year in Review

**January 5, 2021**
*Hinshaw Privacy & Cyber Bytes*

*>> Sign up for our Data Privacy & Cybersecurity mailing list to receive important insights concerning cybersecurity and data privacy laws and developments, along with best practices, and compliance tips.*

A year full of firsts, 2020 introduced a number of new consumer data privacy protection laws. While the California Consumer Privacy Act (CCPA) is one of the most well-known, other states have also adopted their own privacy laws and requirements for businesses to implement and maintain reasonable security measures. We highlight significant data privacy developments and trends from 2020 below.

## California

The groundbreaking CCPA went into effect in January 2020. Similar to the E.U. 's General Data Protection Regulation, the CCPA created a number of privacy rights for California consumers, as well as obligations for businesses that collect and process personal information. The CCPA's implementing regulations were approved in August 2020. The California Attorney General (AG), however, proposed modifications to the regulations in October and in December 2020. Although the AG has yet to commence a CCPA enforcement action, dozens of lawsuits purporting to state a claim pursuant to the Act's limited private right of action have been filed.

While businesses remain focused on the legal and operational challenges of complying with the CCPA, California residents voted in November to approve another privacy law, the California Consumer Privacy Rights Act (CPRA). In addition to modifying the CCPA, the CPRA further expands consumer privacy rights. One significant addition is the Right to Rectify, which requires covered business to use "commercially reasonable efforts" to correct personal information upon receiving a verifiable consumer request. Most of the CPRA's provisions take effect on January 1, 2023, but its expanded Right to Know provision will look back to personal information a covered business collected after January 1, 2022. The CPRA also creates a statewide privacy agency that will be charged with enforcing privacy laws. This likely will lead to increased enforcement actions for privacy violations in California.


### Attorneys

Heather D. McArn

Judith A. Selby

Joanna L. Storey


### Service Areas

Data Privacy & Cybersecurity



©2021 Hinshaw & Culbertson LLP

## New York

A proposed amendment to New York's Civil Rights Law would create criminal liability for certain privacy violations, and the proposed It's Your Data Act would create CCPA-like consumer privacy rights but with a broader private right of action. The proposed New York Privacy Act (NYPA) drew considerable attention in 2019 due to its creation of a fiduciary obligation on data controllers, but stalled in the New York State Senate in early 2020. The New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which amended New York's breach notification law and required covered businesses to implement and maintain reasonable security measures, went into effect in March 2020.

In July, the powerful New York State Department of Financial Services (DFS) initiated its first enforcement action for alleged violations of its first-in-nation 2017 cybersecurity regulation. Three months later, DFS released a comprehensive investigative report of the July 2020 Twitter hack. In September 2020, New York State's Attorney General announced the $39.5 million settlement of the 2014 Anthem Inc. data breach.

## Texas

The Texas Privacy Protection Advisory Council issued a report in September 2020, which described recent state legislative activities and various privacy and compliance challenges. The Council provided the following recommendations for proposed privacy laws against that backdrop:

- Process for ensuring that all state agencies are adhering to privacy standards, and policies are continually updated to reflect new technologies, business practices, and risks.
- Proposals should consider a new and appropriate balance between additional consumer privacy protections and data security within a fair regulatory/compliance privacy framework.
- Proposals should consider the impact to highly regulated data, like health information or banking data, and how those proposals compliment applicable federal law.
- Legislation should be written broadly enough to allow the adoption of new technology and business standards.
- Proposals should consider existing laws in Texas and other states in order to not conflict.
- Texans have the right to know how their personal information is being used and the Legislature should consider ways to strengthen that right.

## Other States

Several bills concerning the protection of biometric information are pending in the Massachusetts legislature, and comprehensive privacy bills were introduced in a number of states, including New Hampshire and Virginia. Although the Washington Privacy Act failed in 2019 and 2020, a new version of the bill likely will be introduced in 2021. Connecticut's Insurance Data Security Law went into effect on October 1, 2020. The Connecticut Insurance Department issued guidance for compliance with the law in July 2020.

## Federal Initiatives

Efforts in support of a comprehensive federal privacy law continue, and a biometric privacy bill—which contains a private right of action—was introduced in the U.S. Senate in August 2020.

In December 2020, the Department of Health & Human Services issued a Notice of Proposed Rulemaking to modify the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The proposed changes would allow patients to obtain their medical records faster and to take notes, videos, and photographs of their personal health information (PHI).

On December 15, 2020, the Office of the Comptroller of the Currency, the Federal Reserve Board and the FDIC issued a notice of proposed rulemaking that would require substantially faster notification of cybersecurity incidents involving banking organizations, expand the list of triggering events, and impose first-of-its kind notification requirements for bank



©2021 Hinshaw & Culbertson LLP

service providers. Specifically, a banking organization would have to provide its primary federal regulator with notice of any "computer-security incident" that rises to the level of a "notification incident" as soon as possible, but not later than 36 hours after, a good faith belief that such incident occurred. A bank service provider would have to notify banking organization customers immediately if it experiences a computer-security incident that could disrupt, degrade, or impair the services it provides for four or more hours.

## BIPA

Class action cases, often culminating in multi-million dollar settlements, continue to be filed for alleged violations of the Illinois Biometric Information Privacy Act (BIPA), which is currently the country's only biometric information privacy law with a private right of action. BIPA claims against high-profile companies like TikTok, Microsoft, and Google, along with massive settlements involving social media giants like Facebook, have garnered the most publicity. It's important to note, however, that BIPA claims have been filed against entities of all sizes. Many BIPA cases have arisen in the employment context, where biometric technologies are used for timekeeping and identity verification functions.

## Canada

In November, Canada's Minister of Information Science and Economic Development introduced legislation to enact two acts, the Consumer Privacy and Protection Act (CPPA) and the Personal Information and Data Protection Tribunal Act (PIDPT), that together would significantly change Canada's privacy laws and their enforcement. The PIDPT would establish a Tribunal to hear appeals of certain decisions made by the Privacy Commissioner under the CPPA and impose penalties for certain contraventions.

The CPPA would replace Canada's long-standing Personal Information Protection and Electronic Documents Act (PIPEDA) and enhance individuals' control over their personal information by creating various rights, including rights to deletion and data portability, and mandate additional requirements concerning notice and obtaining consent. CPPA authorizes hefty penalties—up to 5% of global revenue or $25 million for certain serious violations—and provides for a private right of action triggered by (1) a finding by the Privacy Commissioner that an organization violated CPPA and the finding was either not appealed or dismissed by the Tribunal established by PIDPR; or (2) the Tribunal made a finding that the organization violated CPPA.

## E.U. Developments

In the European Union, a directive allowing representative collective actions for alleged violations of E.U. law in a broad range of areas, including data protection, was recently endorsed. Although the Directive falls short of authorizing U.S.-style class actions, the chances of facing a collective action on behalf of E.U. consumers will likely increase.

The July 2020 ruling in *Schrems II* by the Court of Justice of the European Union invalidating the E.U.-U.S. Privacy Shield—a mechanism that permitted the transfer of personal information from E.U. member states to the U.S.—has created significant uncertainty with regard to international data flows. The risk of unintentional noncompliance has been increased due to open issues concerning how. Before transfer, organizations should assess the adequacy of data protections provided by third countries. In December 2020, E.U. regulators issued recommendations for "supplemental measures" that organizations should consider to customize compliant data transfers. The regulators also proposed updates to Standard Contractual Clauses, which would support a wider range of data transfer relationships and address the issue of government access to data (requiring, for example, a data importer's commitment to notify the data exporter and challenge any government access request).

Following Brexit and the U.K.'s departure from the E.U. on January 1, 2021, data flows between the U.K. and the E.U. can freely continue. A Trade and Cooperation Agreement reached at the end of December provides a six-month "bridging mechanism" which will protect the free flow of data until a formal adequacy decision under the GDPR can be obtained. While it is widely believed that U.K. adequacy will be achieved, the Agreement empowers a Partnership Council to supervise operation of the Agreement and make recommendations and solutions with respect to transfer difficulties or an



©2021 Hinshaw & Culbertson LLP

adequacy challenge. As of January 1, 2021, the GDPR no longer applies to the U.K. but rather is saved into U.K. domestic law and renamed the "U.K. GDPR." The current E.U. transfer framework—including existing adequacy decisions and standard contractual clause as a transfer mechanism—is preserved in the U.K. GDPR, allowing for data flows from the U.K. to third countries to continue in the same way as before.

In December 2020, the E.U. regulators proposed a directive requiring companies in previously designated essential and important sectors, including energy, banking, financial market infrastructures, health, and digital infrastructure, to implement measures to improve cyber resilience. The maximum fine for non-compliance is 2% of global turnover. Before it can go into effect, the proposal must be approved by member states and the E.U. Parliament.

## What to Watch For in 2021

While the Biden-Harris Transition official website does not specifically address how the incoming administration plans to tackle consumer data privacy protection, on December 17, 2020, President-elect Biden issued a statement in response to the recent massive cybersecurity breach affecting the federal government and private sector that the administration "will make cybersecurity a top priority at every level of government." When serving as California's Attorney General, Vice President-elect Harris was a strong advocate for consumer data privacy protection and issued a series of recommendations for businesses, including Making Your Privacy Practices Public and the California Data Breach Report. Thus, it would not be surprising to see a push for comprehensive federal data privacy and security legislation.

There is no crystal ball to predict what lies ahead in the 117th U.S. Congress. Consumer privacy protection state legislation on the horizon includes Arizona SB 1614 (consumer data privacy), Arizona HB 2729 (data security standards), Illinois SB 2263 (data privacy act), Illinois SB 2330 (data transparency and privacy act), Illinois HB 5603 (consumer privacy act), Maryland HB 0784 (consumer protection), Minnesota HF 3936 (consumer data privacy act) and the Washington Privacy Act of 2021.

*>> Sign up for our Data Privacy & Cybersecurity mailing list to receive important insights concerning cybersecurity and data privacy laws and developments, along with best practices, and compliance tips.*

*The views expressed in this article are those of the author and may or may not reflect the views of AEGIS Insurance Services, Inc.*



©2021 Hinshaw & Culbertson LLP