Cybersecurity Policy Report
Strategic Perspectives

Wolters Kluwer

December 10, 2021

Rapid Evolution of Privacy and Cyber Laws Expected to Continue in 2022

By Tony Foley

With 2021 in the rear view mirror, having seen the enactment of a plethora of privacy and cybersecurity requirements at the state level, the pace of change is likely to continue, and perhaps accelerate in 2022, creating significant—and disparate—compliance obligations on businesses that collect, process and use personal information. In the meantime, enactment of a federal privacy law doesn't seem significantly more likely than it has been in the last several years, while on the international front, data protection authorities have stepped up their efforts to enforce comprehensive data protection regimes like the EU General Data Protection Regulation (GDPR), particularly in areas such as cross border transfer requirements and privacy and data protection provisions applicable to big tech companies.

This article takes a look back at the most important developments from the past year, and looks ahead to what experts expect to see in 2022.

California, Virginia, Colorado Lead the Way as States Pick Up the Privacy Pace

The California Consumer Privacy Act (CCPA), which was enacted in 2018 and took effect in 2020, was the first comprehensive privacy and data protection legislation enacted in the U.S. Nearly two years, and many bumps, later, Golden State voters approved the California Privacy Rights Act (CPRA) in November 2020, which amended the CCPA in many respects, perhaps most notably by establishing a dedicated state agency (the California Consumer Privacy Agency or CPPA) to oversee compliance with the law and conduct enforcement activities.

2021 comprehensive laws. During the 2021 legislative session, more than 20 states proposed comprehensive legislation, but as the dust settled on state sessions, only two were able to enact new laws. In March, Virginia Gov. Ralph Northam (D) signed the Virginia Consumer Data Protection Act (CDPA) into law, and Colorado followed suit in July when Gov. Jared Polis (D) signed the Colorado Privacy Act (CPA). As noted, many states (most notably Washington, Florida, and New York) worked diligently to pass comprehensive laws in their legislative sessions but were unable to push them across the finish line. Sources indicate that legislators from a number of states that failed to enact privacy legislation plan to reintroduce proposed legislation in 2022, while in other states, privacy legislation that was pending on adjournment (like the proposed Ohio Personal Privacy Act, introduced in July) will carry over to the 2022 session.

While Virginia's CDPA, which will take effect on January 1, 2023, and Colorado's CPA, which will take effect on July 1, 2023, contain many of the same elements as California's CCPA as amended by the CPRA, there are differences. For example, the California laws reach a wide range of businesses, while Virginia's and Colorado's apply to a narrower segment of data controllers and processors. In addition, there are subtle, but substantial, differences in each law's enforcement requirements. For example, California has an explicit right to a private cause of action for violations under specified conditions, while no such right exists under the new laws in Virginia or Colorado. On the other hand, a specified period to cure a violation before enforcement proceeding may be initiated is available both under the Virginia law (30 days) and the Colorado law (60 days, at least through January 1, 2025, when the cure provision will lapse).

These differences, and the many others that exist, make it imperative that businesses carefully review their compliance mechanisms to ensure that their data collection and processing activities are conducted in accordance with all necessary requirements. Businesses that have developed plans to comply with the CCPA (and the GDPR, for that matter) certainly have a leg up on establishing the appropriate safeguards, but the California amendments, and Virginia and Colorado provisions, almost certainly will require significant adjustments.

Other activity and aggressive adoption of model law. While most outsiders were focusing their attention on the various comprehensive bills outlined above, legislatures quietly enacted a number of less flashy, but nonetheless important privacy provisions, many of them relevant to specific industries.

The ongoing adoption of the model Insurance Data Security Law by states continued unabated in 2021, as the number of states adopting the model provisions doubled, to 18 states total. The model law requires insurers regulated by an adopting state to implement and maintain a comprehensive data security program and to notify consumers and state regulators of any cybersecurity incident meeting statutory requirements.

Other enactments of note included the following:

- Both Utah and California enacted a Genetic Information Privacy Act. In each case, the law requires direct-to-consumer genetic testing companies to provide information to consumers on their collection and processing activities, restricts the manner in which such information may be disclosed, and provides data security and deletion requirements. Meanwhile, Louisiana enacted a law prohibiting specified insurers from requesting an individual or family member to take a genetic test or to use genetic information for underwriting purposes.
- In Nevada, existing law requires operators of websites collecting personal information about consumers in the state to establish a verified address through which consumers may request that their information not be sold. A law enacted in June extends these requirements to "data brokers," which are defined as persons primarily in the business of purchasing covered information about Nevada consumers from operators and other data brokers and selling such information. The new law also provides for a 30-day cure period applicable to operators and data brokers.
- Connecticut and Texas each made significant changes to their breach notification laws. Connecticut expanded its definition of personal information to include a variety of additional

categories of information, and shortened the time period to notify of a breach from 90 to 60 days, while in Texas, businesses required to make a notification of a breach must include the number of affected residents in their notice to the Attorney General and must maintain a list of breach notifications on its website.

- In Oregon, a new law establishes a private cause of action for improper disclosure of private information in cases where a plaintiff can show by a preponderance of the evidence that the defendant knowingly made the disclosure with intent to stalk or harasses the plaintiff. The law provides for economic, noneconomic and punitive damages, and injunctive relief.

What to expect in the states in 2022. With states continuing to press for the enactment of additional privacy provisions, businesses should be prepared to deal with a dizzying array of requirements. "New state laws will impact businesses by forcing companies to consider the role of compliance in their organizations," said Jared Miller, Esq. and Dr. Jim Castagnera, partners at Portum Group International, a cybersecurity and data privacy consulting firm based in Philadelphia. "Having trained compliance professionals helping to oversee a data privacy or cybersecurity program will be the best way for businesses to comply with the confusing and contradictory privacy landscape we will see in the U.S."

Jena Valdetero, Co-Chair of the U.S. Data, Privacy and Cybersecurity Practice at Greenberg Traurig, agreed that businesses will face unique challenges moving forward. "The primary impact is likely to be increased cost of compliance of the laws and a decision by more companies to adopt a jurisdiction-agnostic privacy program in anticipation of similar laws passing in the future as privacy is only getting more, not less, regulated," she said.

"[B]usinesses of all sizes, and in all industries, have had to become much more proactive in addressing their cybersecurity risks," added Hillard M. Sterling, partner at Clausen Miller, P.C. "It is no longer sufficient – if it ever was – for businesses to take a 'cookie cutter' approach to their pre-breach protective measures. Rather, state laws and regulations require specific and expansive cybersecurity measures."

A new model law to watch. While legislators in a number of states have signaled that they plan to reintroduce comprehensive legislation next year, another potential avenue for expansion of state privacy law opened with the approval of the model Uniform Personal Data Protection Act (UPDPA) by the Uniform Law Commission in July. While the UDPDA shares some features with current state data protection laws, it is designed in a manner that attempts to find a middle ground that most states have been unable to achieve, providing basic consumer protections while avoiding some of the perceived costs of regulation and compliance inherent in existing state provisions and providing the opportunity for greater conformity across the states.

[Perkins Coie LLP attorney Kim Ng has provided an excellent overview of the UPDPA, including an analysis of the significant difference between the model law and the California, Virginia, and Colorado laws.]

In October, the District of Columbia became the first jurisdiction to introduce the UPDPA in October, and experts predict that it will be a popular option come January. "We expect states will start to

implement the [UPDPA]," said Mr. Miller, and Dr. Castagnera. "While larger states with data-savvy legislatures, such California or New York, will continue to do their own thing, uniform laws are a great way for smaller states which might be newer to data protection to effectively protect their citizens' privacy rights." Mr. Sterling said that he expects some states to introduce the UPDPA, but added that "unlike other uniform laws, many states likely will forego the UPDPA and instead model their laws around other states' existing cybersecurity laws, such as those in California and New York. Other states will borrow from the UPDPA yet forego pieces of the proposed law, particularly with regard to its more controversial components such as its reliance on existing consumer-protection laws for enforcement."

Congress Still Stalled on Adoption of Federal Privacy Standard

As is the case most years, members of Congress on both side of the aisle lamented the absence of a federal privacy regime in the U.S. and some introduced bills designed to address the gap.

Comprehensive federal legislation. Primary among the proposed comprehensive legislative proposals introduced in 2021 are S. 2499, the SAFE DATA Act, sponsored by Sen. Roger Wicker (R. Miss.), and S. 1494, the Consumer Data Privacy and Security Act (CDPSA), sponsored by Sen. Jerry Moran (R.-Kan.).

Both bills would establish specified individual rights and would impose obligations on businesses that collect and process personal information. Importantly, on the enforcement side, both bills specify that they will preempt any state privacy and data security laws other than data breach notification laws, and neither bill provides for a private cause of action for violations.

Narrower proposals. Additional legislative proposals aim to enact targeted privacy provisions, many of them related to privacy concerns arising from the COVID-19 pandemic. Among the bills receiving the most attention are the following:

- H.R. 1816, the Information Transparency and Personal Data Control Act, sponsored by Rep. Suzan DelBene (D. Wash.), which would require the opt-in consent for the use of a consumer's sensitive personal information and would specify that privacy policies be presented in plain English;
- S. 919, the Data Care Act, sponsored by Senator Brian Schatz (D.-Haw.), which would require online service providers handling identifying data to secure it from unauthorized access, refrain from using it in a harmful manner, and not disclose the data to another party unless the party is bound to the same obligations;
- S. 1667, the Social Media Privacy Protection and Consumer Rights Act, sponsored by Sen. Amy Klobuchar (D.-Minn.), which would grant users of online platform operators the right to opt out of data collection and tracking and would require operators to establish a privacy and security program;
- S. 2290, the Data Broker List Act, sponsored by Sens. Shelley Moore Capito (R.-W.Va.), Cynthia Lummis (R.-Wyo.) and Gary Peters (D.-Mich.), which would create a data broker registry and require data brokers to implement comprehensive information security systems; and
- S. 2875, the Cyber Incident Reporting Act, sponsored by Sen. Peters, one of several pending bills that would require critical infrastructure operators to report attacks and ransomware payments, which recently cleared the Senate Homeland Security and Governmental Affairs Committee.

In addition, some enacted federal legislation did impact on cybersecurity and privacy, including H.R. 3684, President Biden's infrastructure bill signed into law on November 15 that includes about $2 billion in cybersecurity funding.

What to expect in Congress in 2022. At present, all of the bills described above remain in committee, and their prospects for eventual passage, save perhaps for the Cyber Incident Reporting Act, are slim. "The question of federal legislation continues to arise year after year, and yet Congress still cannot seem to agree on the terms of the bill," said Ms. Valdetero. "The issue of whether a federal law will preempt state laws, thereby replacing stricter laws, remains a point of contention, as does whether a federal privacy law should provide for statutory damages to individuals who successfully argue in court that the law was violated." Mr. Sterling of Clausen Miller agreed, particularly on the preemption issue, adding that "[s]tates are increasingly active in the cybersecurity arena, and they will not yield their jurisdiction lightly."

However, Mr. Miller and Dr. Castagnera still see the potential for a federal standard to eventually be enacted. "We don't believe that federal privacy law is dead," said Mr. Miller and Dr. Castagnera. "Some of the inaction is classic Congressional partisan gridlock and some of it is data controllers lobbying to keep any federal law weak." They added that the impact of Rep. Nancy Pelosi's (D.-Cal.) potential retirement or resignation of the Speaker's chair may convince Democrats to move on the issue of federal preemption, which as noted, has been a major roadblock to progress.

Administrative Activity Accelerates

Meanwhile, federal regulators have stepped up their enforcement activities related to privacy and data protection, and have implemented new guidance and procedures spurred on by the exponential increase in ransomware attacks and other cybersecurity incidents.

Executive orders. The Biden Administration wasted little time establishing itself in the cybersecurity area, issuing Executive Order 14028 in May. The EO leveraged the federal government's purchasing power to insist that its suppliers observe the most up-to-date security practices, disclose any gaps in those practices, and quickly tell the government about any significant breaches. The order specifies required actions by a host of regulatory agencies, many but not all of which have been completed, although some agencies have more time for implementation prior to a final deadline.

FTC and SEC enforcement actions. The FTC continued a trend in 2021 that has seen the agency pursue an increased number of actions related to privacy and data security, staring in February with the finalization of a settlement with Zoom Communications over allegations that the company misled consumers about the level of security it provided and compromised the security of the hardware of some users. The agency focused on imposing greater accountability with respect to data security, including a settlement with emergency travel services provider SkyMed International for its failure to properly secure sensitive customer data, as well as enforcement of violations of the Children's Online Privacy Protection Rule (COPPA) (see the settlement with children's app developer Hyperbeard, LLC, which was hit with a $150,000 fine) and actions against companies

that engage in illegal telemarketing (see the settlement against Alcazar Networks Inc. concerning its facilitation of millions of illegal robocalls).

The SEC also issued a number of enforcement actions in 2021, mostly tied to the failure of regulated businesses to properly secure data in their possession, leading to data breach incidents. Among the most noteworthy of these actions was a sanction against eight firms, in three separate actions, based on failures in their cybersecurity policies and procedures. Fines imposed in the case totaled $750,000.

TSA cyber directives. The Transportation Security Agency (TSA) issued several directives in 2021 aimed at combatting these incidents, including two pipeline security directives, one from May and the other from July, that require owners and operators of TSA-designated critical pipelines to report cybersecurity incidents to the TSA and to implement specified protections against cyber intrusion. TSA followed that up in December with the issuance of additional security directives applicable to rail carriers and other surface transportation providers establishing similar requirements.

Other agencies. In other administrative activity, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have issued the first three parts of a 4-part series of guidance on security guidance for 5G cloud infrastructures (available on CISA's 5G resource page). The guidance is designed to assist service providers and system integrators building 5G cloud infrastructure with respect to issues like secure isolation of network resources and data protection. The Department of Homeland Security (DHS) also issued a binding operational directive in November that is directed at software and hardware found on federal information systems and establishes review and remediation of procedures designed to reduce the significant risk of known exploited vulnerabilities.

And most recently, the Office of the Comptroller of the Currency (OCC), the Federal Reserve, and the FDIC each issued regulations requiring banking organizations regulated by the respective agencies, and their service providers, to report specified data security incidents within 36 hours.

What to expect in 2022. Most indications are that the FTC, in particular, will explore the promulgation of privacy and data security regulations, as opposed to its current reliance on enforcement actions under Section 5 of the FTC Act. At a February conference, FTC Commissioner Christine Wilson said that rulemaking may be necessary. "I would hope that Congress will act, but if Congress doesn't act, maybe we do spend that time," she said. "It is the second best—it's not even the second best, it's the third best [option]—but maybe that's what we need to do in order to bring certainty and predictability for businesses and transparency for consumers." And in May, then-Acting FTC Chair Rebecca Slaughter, who has since been replaced as Chair by Commissioner Lina Khan, indicated that she intended to pursue additional rulemaking to tackle concerns about data and privacy protection. In August, a group of more than 20 consumer advocacy organizations sent the FTC a letter asking the agency to initiate rulemaking designed to protect civil rights and privacy in data-driven commerce.

"Until there is a uniform federal privacy law, we will see regulators try to work with the power they have to solve the problem of data protection in the United States," said Mr. Miller and Dr. Castagnera, who also expect a push from agencies like the Treasury Department, Veterans'

Administration, and HHS, which have a broader mandate under current regulations to enforce data protection and cybersecurity laws than the FTC and SEC. Ms. Valdetero, citing the recently enacted banking regulations, added that "[w]e are definitely seeing more activity from state and federal regulators in the areas of both privacy and security compliance in the form of new regulations and enforcement activity."

Globally, EU Guidance and Enforcement, and China, Take Center Stage

On the international front, EU lawmakers and regulators were active in adopting new guidelines for data controllers and processors, particularly with respect to cross-border transfers. Since the invalidation of the EU-U.S. Privacy Shield transfer mechanism in the *Schrems II* decision, significant uncertainty has reigned in this area.

New SCCs, other guidance. In June, the European Commission adopted two sets of standard contractual clauses (SCCs) that reflect updated GDPR requirements and also take into account the *Schrems II* judgment. In particular, the new SCCs emphasize that in order to comply with *Schrems II*, supplementary measures such as encryption often will be required to justify cross-border data transfers, particularly from the EU to the U.S. [Experts at Ogletree Deakins provided a comprehensive review of the new SCCs shortly after their adoption that is of particular interest to employers.]

In November, the European Data Protection Board (EDPB) issued guidelines discussing the interplay between the application of the territorial scope provisions of the GDPR Art. 3 and GDPR Chapter V provisions governing cross-border transfers of data. The guidelines are designed to assist data controllers and processors in the EU to identify whether a particular act of processing constitutes a transfer to a third country or to an international organization and therefore require compliance with the requirements of Chapter V.

Enforcement. EU data protection authorities also made a splash in enforcement, particularly in their supervision of the data collection and processing activities of major tech companies, often imposing sanctions in the millions of dollars. Among the most talked about enforcement actions were the following:

- In January, Datatilsynet, the Norwegian data protection authority, fined app company Grindr LLC $11.7 million for its failure to comply with GDPR consent requirements.
- In February, the Italian Competition Authority fined Facebook Ireland Ltd. and Facebook Inc. almost $8.5 million based on the companies' failure to comply with a previous order regarding unlawful processing of personal information.
- Amazon disclosed in an SEC filing in July that the Luxembourg National Commission for Data Protection intended to impose a fine of nearly $887 million against the company based on a finding that its data processing was not GDPR-complaint (Amazon has subsequently filed an appeal of the decision).
- The Irish Data Protection Commission (DPC), which serves as the primary regulator for most big tech companies, issued a fine of $267 million against WhatsApp in September, finding that the company failed to properly discharge its transparency obligations. In October, the same body

issued a draft decision against Facebook Ireland for between $31 million and $42 million for similar violations (a decision immediately dismissed by EU privacy watchdog None of your business (noyb) as a "GDPR bypass," since the DPC did not expressly reject Facebook's contention that its processing was necessary for the fulfillment of a contract, but rather concluded that the fine was justified by Facebook's lack of transparency.

- In November, the UK Information Commissioner's Office (ICO) announced its provisional intent to impose a fine of $22.5 million against software giant Clearview AI because of the company's failure to comply with a variety of UK data protection requirements (although a final determination is not expected until mid-2022).

Chinese PDPL China also was active in 2021, adopting both a data security law, which took effect on September 1, and the Personal Data Protection Law (PDPL), which took effect on November 1. The PDPL is modeled after the GDPR in many respects, including its extraterritorial reach to businesses not located in China, and contains specified data subject rights and controller and processor obligations similar to GDPR requirements. That said, there's still uncertainty about the impact that the PDPL will have outside of China. "Because China's tech landscape exists unto itself, we don't foresee the PDPL having a big impact in the U.S. and Europe," said Mr. Miller and Dr. Castagnera of Portum Group International. "The PDPL will be impactful in the countries China is developing, such as Ethiopia and Nigeria, which might model their own data protection and cybersecurity regimes on the PDPL." Ms. Valdetero of Greenberg Traurig added that "China's new law will pose new challenges that will likely exacerbate an already tense economic relationship with the United States."

What to look for in enforcement in 2022. The apparent increase in enforcement activity contrasts sharply with complaints in prior years that the GDPR, while providing robust protections for individuals, lacked teeth. Most observers believe that EU DPAs will continue to move aggressively to enforce the provisions of the law.

On cross-border transfers, while there seems to be consensus on both sides of the Atlantic on the need for an EU-U.S. transfer mechanism, progress has been slow. "Privacy Shield II or something like it is almost certainly in our future, but whether it addresses the concerns raised in *Schrems* II is a big 'if,'" said Ms. Valdetero. "Right now, companies are doing the best they can to adapt to the ever changing guidance from regulators while still trying to continue doing business across borders." Meanwhile, Mr. Miller and Dr. Castagnera see the potential for European regulatory activity to influence any new cross-border regime. "U.S. and EU officials want a Privacy Shield II. Whether Shield II will go the way of the Safe Harbor or Shield I is another question," they said. "Continued action from European regulators will drive the language of privacy in a European direction."