Articles + Publications | January 4, 2022

The 2021 Year in Review and What to Expect in Data Security in 2022

WRITTEN BY

Matthew R. Cali | Angelo A. Stio, III

This article was originally published on DATAVERSITY and is republished here with permission.

This year saw a number of significant changes on both the state and federal levels with regard to data privacy and data security. These changes reflect the increasing focus on the digital landscape to which the global economy has shifted and emphasized a much sharper focus on protecting sensitive information. Indeed, the significance of having strong cybersecurity regulations was emphasized from the top down in the United States, including an emphasis on improving and updating cybersecurity defenses and protections for federal government networks, as outlined in President Biden's May 12, 2021 Executive Order on Improving the Nation's Cybersecurity. This article highlights the legislative and litigation developments in 2021 and discusses what may lie ahead in 2022 for businesses that collect, process, and store sensitive information.

Federal Legislative Developments in 2021

The Department of Justice (DOJ) launched a Civil Cyber Fraud Initiative that uses the False Claims Act to pursue cybersecurity fraud by government contractors and grant recipients. The initiative holds contractors to a higher standard of data protection, ensures companies follow rules and invest in meeting cybersecurity requirements, reimburses the government and taxpayers for losses incurred when companies fail to satisfy their cybersecurity obligations, and improves overall cybersecurity practices to benefit the government and American public. This initiative also provides whistleblower status to private parties assisting the government in identifying and pursuing fraudulent conduct, and permits whistleblowers to share in any government recovery.

Moreover, the Federal Trade Commission (FTC) issued changes to the Gramm-Leach-Bliley Act's Standards for Safeguarding Customer Information. These changes include a requirement for non-banking financial institutions to develop, implement, and maintain a comprehensive system to secure their customers' data. The so-called Safeguards Rule also includes revisions that put more specific criteria for the types of data security protections financial institutions must have in place.

These data protection criteria include securing data with encryption and controlling access through multifactor authentication, as well as requiring financial institutions to explain the safeguards used to distribute process, access, store, transmit, and use customers' personal data. Moreover, financial institutions now need to appoint a "single qualified individual" to oversee the information security program and report to the organization's board or senior officers on the information security program on a periodic basis. This amendment was approved on October 27, 2021, and was motivated by a number of noteworthy data security and privacy incidents that occurred in the

financial sector over the past few years.

In addition, on October 27, 2021, the FTC announced a proposal to require financial institutions to report security incidents to the Commission electronically through the FTC's website. Under the proposal, financial institutions would be required to notify the FTC of security events where misuse of customer information has occurred or is reasonably likely to occur and where at least 1,000 consumers have been or may reasonably be affected by the incident. Commentators now have 60 days from the date of publication of the notice to submit comments on the proposal.

The Department of Homeland Security through the Transportation Security Authority (TSA) also announced two cybersecurity directives for critical pipeline owners and operators in the wake of the Colonial Pipeline cyber attack. These two directives require certain critical pipelines that transport hazardous liquids and natural gas to implement a number of protocols to protect against intrusions and cyber attacks. These directives show a public-private union aligned to protect critical infrastructure capabilities from interference to preserve the integrity of those services keeping America running every day.

Congress began seriously considering a number of bills to strengthen the Cybersecurity and Infrastructure Security Agency (CISA). Various bills and proposals were introduced, ranging from the most extreme by Senator Mark Warner requiring notice of potential cybersecurity intrusions to CISA within 24 hours of discovery coupled with daily civil penalties of up to 0.5% of an entity's prior year's gross revenue, to more scaled-down versions such as that Senators Gary Peters and Rob Portman's proposal, which provides 72 hours to notify CISA of a cybersecurity intrusion with no civil fines or penalties. Several other proposals have also been discussed, including an amendment to the National Defense Authorization Act to provide rulemaking authority to the CISA director to establish procedures and protocols for reporting cybersecurity intrusions for defined covered entities, and proposals targeting ransomware. Despite the different proposals offered, Congress's message is clear – cybersecurity legislation is on the horizon.

State Legislative Developments in 2021

At least 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity. A number of bills were passed and enacted into law, including California expanding the definition of "personal information" in its data breach law to include genetic data [1] and passing the Genetic Information Privacy Act governing direct-to-consumer genetic testing companies and their vendors[2] and Connecticut enacting "An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses," which provides a limited safe harbor for certain entities from punitive damages if they maintain and comply with a written cybersecurity protocol that conforms to an industry-recognized framework. [3] Other states such as Texas also enacted changes. Texas increased its notification requirements for those suffering data breaches and is now also publicly publishing a list of data breaches on the Texas Attorney General's website. [4]

What to Expect in 2022

Here's a look at what's next for data security:

1. Implementation of initiatives and rules passed in 2021: With the Executive Branch expressing a renewed

focus on cybersecurity, we can expect that the DOJ and FTC will begin implementing and enforcing their newly minted authorities. Regarding the DOJ's Civil Cyber Fraud Initiative, we can expect government contractors to take action by formalizing and implementing cybersecurity protocols to comply with government regulations and minimize the risk for a breach or intrusion. Moreover, with a monetary incentive for whistleblowers, we can expect individuals within such organizations to be proactive in notifying government authorities of any deviations from industry standards. This could result in an increase in government investigations, enforcement, and potential litigation.

Additionally, while the FTC's Safeguards Rule goes into effect in 2021, a number of key requirements of the rule are effective one year from the date of passing. Thus, many financial institutions and related entities will similarly need to implement compliant protocols and procedures to ensure compliance once these rules go into effect. We can expect engagement with legal counsel to provide guidance to these institutions to ensure regulatory compliance. As there usually are, we expect laggards in the industry to serve as the "guinea pigs" of the FTC's enforcement of the Safeguards Rule changes. This may yield investigations, penalties, and possible litigation for violators.

2. Congress will continue to discuss federal cybersecurity legislation: With the numerous large-scale cyberattacks and threats in 2021, and the increasing expectation of additional cyberattacks, we can expect cybersecurity to become a primary issue in Congress. Because the vast majority of American infrastructure is now tied to the Internet of Things, the risks associated with cyberattacks are not just time and money, but potentially lives. The Colonial Pipeline hack was just a small taste of the potentially devastating impact a large-scale cyberattack could have on the United States' infrastructure and the American public. Congress knows it must act to ensure companies, particularly those involved in infrastructure, are protected and institute a certain degree of defenses to thwart potential bad actors.

After a year in which a number of proposed bills and proposals involved a wide range of cybersecurity requirements, we expect a vote on a bill that could require cybersecurity and data protection policies and protocols to be required for certain organizations. [5] This could involve both preventative and remedial requirements for companies that provide critical infrastructure services to the American public. While this will require a degree of cooperation with private corporations, given the life or death risk associated with cyberattacks on these industries, legislation will likely be enacted in the next year. Corporations in these industries should rely on legal counsel in interpreting and complying with any federal legislation enacted to ensure compliance, as there will not only be requirements and possible penalties at the federal level but also at the state level.

3. More states to expand data security and privacy laws: As more personal data becomes placed in commerce, particularly biometric and genetic data, we can expect a number of states to follow California's lead and expand their definitions of what is considered protected "personal information." The growth of ancestry DNA programs, DNA and RNA testing, and other forms of medical tests have resulted in biometric data entering the stream of data corporations maintain for business purposes. To prevent this intimate personal information from falling into the hands of malicious actors, we expect more states to pass similar laws to expand the definition of personal information to include biological and genetic material as California did this past year. This will subject additional businesses and entities that maintain this sensitive data to additional scrutiny.

Additionally, states may also follow Connecticut's lead in expanding their safe harbor for businesses that have

cybersecurity policies and protocols in place in the event there is a data breach or cyber attack. This positive reinforcement from states may motivate businesses to proactively address their cybersecurity policies to ensure they are industry compliant. Cyberattack prevention will become the focus in many states because, despite the benefits of strong remedial requirements, prevention is the key to avoiding damage to the public.

Finally, we may see more states implement more stringent notification and reporting requirements. Just as Texas amended its data breach notification requirements to broaden the information affected entities must provide to the Texas Attorney General when reporting a data breach and will now publish a list of reported data breaches [6], additional states may likely continue the trend. Given the fragmented nature of each state's reporting and notification requirements, we may begin to see a trend towards uniformity as each state continues to amend and mold their data protection statutes to keep up with the states at the forefront of addressing the ever-evolving digital landscape.

4. Litigation arising from the new rules, laws, and regulations: After such a transformative year involving the passing of new laws, regulations, and initiatives, there will be litigation both arising from the new requirements and challenges thereto. Private corporations may levy constitutional challenges on Congress's ability to regulate their handling of personal information should Congress enact a federal cybersecurity or data breach statute. There also may be a rise in employment-related retaliation cases by whistle-blowers against noncompliant government contractors. Finally, with more states amending and expanding their data protection and privacy statutes, we can expect some entities resistant to implementing cybersecurity protocols to fall victim to not only an underlying cyberattack, but regulatory action and class action lawsuits by impacted individuals. For businesses, compliance and risk mitigation will be vital to defending their cases.

---

[1] Cal. Civil Code § 1798.82(h)(1)(H)

[2] California Senate Bill 41 (effective January 1, 2022)

[3] H.B. No. 6607; Public Act No. 21-119

[4] H.B. 3746, amending Tex. Bus. & Com. § 521.053

[5] The TSA has already begun implementing cybersecurity regulations on pipelines in the wake of the Colonial Pipeline attack. If Congress does not act on these proposed bills, we foresee the TSA may do so, focusing on rail and air travel operators.

[6] Texas House Bill 3746

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber