Your Privacy New Year's Resolutions: What You Need to Know for 2022

To kick off the countdown to World Data Privacy Day, we want to provide businesses, organizations and individuals with a few important reminders going into 2022. With the increase in data privacy laws and enforcement, data privacy best practices should be imperative New Year's resolutions for organizations. Here are some important statutory and regulatory privacy issues and topics that businesses should keep in mind heading into the new year:

CPRA Lookback

Although the California Privacy Rights Act (CPRA) does not officially go into effect until Jan. 1, 2023, its lookback period began on Jan. 1, 2022. As a reminder, on Nov. 3, 2020, California voters approved Proposition 24, also known as the CPRA, which was designed to supplement and amend the California Consumer Privacy Act (CCPA). Under the CPRA lookback period, that data collected during 2022 is subject to the terms of the CPRA starting in 2023. This means that any personal information that your business may collect throughout 2022 should be collected in compliance with CPRA on Jan. 1, 2023 if you intend to use it from that point on, and businesses must disclose it in a consumer right to know request. As a result, all covered businesses should bring their policies and collection practices into compliance with the CPRA as soon as possible.

Biometric Information Privacy Act

Over the last couple of years, class action lawsuits under the Illinois Biometric Information Privacy Act of 2008 (BIPA) have steadily increased and continue to bring about groundbreaking data privacy litigation. BIPA was the first law of its kind, and comprehensively regulates business' collection of biometric data. An important component of BIPA is its broad private right of action, which allows "any person aggrieved by a violation of [the] Act" to sue for large damage amounts as well as fees, costs, injunctive and other relief. Between its passage and August of 2021, this private right of action enabled over 750 class action lawsuits to be filed across federal and state courts and have led to substantial settlement amounts. In 2022, there will likely be an increase in class action filings under BIPA, specifically concerning biometric information collection as part of COVID-19 health screenings. Recent litigation has increased individual rights as well, including issues involving statute of limitations and evidentiary standards. As a result, businesses are facing greater exposure to liability for failing to follow BIPA regulations.

BIPA requires any private entity in possession of biometric information to: (i) develop a written policy; (ii) inform the owner of the biometric information in writing about the purpose for collecting the information and the length of time it will be stored; (iii) obtain written consent for the collection and storage of the data; and (iv) refrain from selling, leasing, trading or otherwise profiting from that biometric information.[1]

So far this year, Maryland, Massachusetts, Kentucky, and West Virginia are considering their own BIPA-like biometric privacy legislation. Given the increased BIPA litigation and biometric privacy law legislative trends developing in other states, businesses should ensure they are in technical and procedural compliance with BIPA provisions as soon as possible.

Massachusetts Written Information Security Plan

When an entity experiences a data breach, important lessons are often learned too late. The 2010 Massachusetts data security regulations require every entity that owns or licenses personal information about Massachusetts'

1 740 ILCS 14/1, et seq.

residents to implement a written information security plan (WISP) that helps safeguard such personal information. Despite this requirement, many covered entities, especially those that do not have a physical presence in Massachusetts, only learn about these regulations when they experience a data breach.

Although the WISP requirement is not new, Massachusetts amended its data breach notification law in 2019 to require businesses to report to the Massachusetts Attorney General its WISP status at the time of the breach. Since Massachusetts does not have a threshold limitation for Attorney General data breach reporting obligations or for the implementation of a WISP, a business wholly located outside of Massachusetts that maintains a small amount of residents' data could be subject to these requirements. Failure to maintain a WISP could lead to increased fines and enforcement penalties for covered businesses.

Massachusetts is not the only state that requires a WISP. As of 2021, numerous other states including Rhode Island, Texas, California and Oregon also had WISP requirements. Given this increased risk of liability, covered businesses should make it a priority to develop, implement and maintain a WISP that complies with Massachusetts' strict data security regulations.

Privacy Risk Mitigation of Vendor Contracts

Vendor risk management helps ensure that third-party vendors, products and services do not disrupt an organization's services or cause financial, reputational or other damage. Many businesses outsource at least part of their services to third-party vendors. As a result, these vendors have access to intellectual property and other sensitive information, including personal information of employees, customers, students or others. As vendors have increased access to important and sensitive information, a business' risk profile for reputational, operational, legal or cybersecurity risk multiplies. Ensuring that the contractual relationship between the parties delineates required compliance mechanisms and data protection safeguards is essential to managing these risks. Given the rise in cyberattacks and the increased regulatory arena of data privacy, it is imperative to review and revise vendor contracts to ensure data protection safeguards are incorporated into agreements.

Vendor contracts frequently include provisions that allocate the majority of risk to the business partner. This includes placing the majority of the cost and risk of a data breach or privacy compliance obligations on the business. These agreements typically include disclaimers for breach damages and limitations on liability for privacy and cybersecurity losses. Businesses should take extra precautions when reviewing vendor agreements and should develop standard data privacy and security terms to ensure vendors sufficiently protect data. Importantly, vendor contracts should consider reporting and response obligations in the event of a cybersecurity incident, including allocation of cost and responsibility for handling any resulting liability. Businesses should also review their cybersecurity insurance policies regarding required vendor diligence and risk assessment. Addressing these risks upfront can lower privacy and cybersecurity risks and streamline compliance efforts moving forward.

For more information or guidance concerning any of the topics in this information memorandum, please contact Amber Lawyer, CIPP/E, Shannon Knapp, CIPP/US, or any attorney in Bond's Cybersecurity and Data Privacy practice.

Thank you to Associate Trainee Dustin Dorsino for his help drafting this information memorandum.

BOND SCHOENECK & KING ATTORNEYS