JacksonLewis

Top 10 Data Privacy & Security Considerations for 2022

While this list is by no means exhaustive, it provides some hot topics for organizations to consider in 2022.

1. State Consumer Privacy Law Developments

On January 1, 2020, the CCPA ushered into the U.S. a range of new rights for consumers, including:

- The right to request deletion of personal information;
- The right to request that a business disclose the categories of personal information collection and the categories of third parties to which the information was sold or disclosed; and
- The right to opt-out of sale of personal information; and
- The California consumer's right to bring a private right of action against a business that experiences a data breach affecting their personal information as a result of the business's failure to implement "reasonable safeguards."

In November of 2020, California voters passes the California Privacy Rights Act (CPRA) which amends and supplements the CCPA, expanding compliance obligations for companies and consumer rights. Of particular note, the CPRA extends the employment-related personal information carve-out until January 1, 2023. The CPRA also introduces consumer rights relating to certain sensitive personal information, imposes an affirmative obligation on businesses to implement reasonable safeguards to protect certain consumer personal information, and prevents businesses from retaliating against employees for exercising their rights. The CPRA's operative date is January 1, 2023 and draft implementation regulations are expected by July 1, 2022. Businesses should monitor CCPA/CPRA developments and ensure their privacy programs and procedures remain aligned with current CCPA compliance requirements. For practical guidance on navigating compliance, check out our newly updated CCPA/CPRA FAQS.

In addition to California developments, in 2021, Virginia and Colorado also passed consumer privacy laws similar in kind to the CCPA, both effective January 1, 2023 (together with the CPRA). While the three state laws share common principles,

including consumer rights of deletion, access, correction and data portability for personal data, they also contain key nuances, which pose challenges for broad compliance. Moreover at least 26 states have considered or are considering similar consumer privacy laws, which will only further complicate the growing patchwork of state compliance requirements.

In 2022, businesses are strongly urged to prioritize their understanding of what state consumer privacy obligations they may have, and strategize for implementing policies and procedures to comply.

2. Biometric Technology Related Litigation and Legislation

There was a continued influx of biometric privacy class action litigation in 2021 and this will likely continue in 2022. In early 2019, the Illinois Supreme Court handed down a significant decision concerning the ability of individuals to bring suit under the Illinois's Biometric Information Privacy Act (BIPA). In short, individuals need not allege actual injury or adverse effect beyond a violation of his/her rights under BIPA to qualify as an aggrieved person and be entitled to seek liquidated damages, attorneys' fees and costs and injunctive relief under the Act.

Consequently, simply failing to adopt a policy required under BIPA, collecting biometric information without a release or sharing biometric information with a third party without consent could trigger liability under the statute. Potential damages are substantial as BIPA provides for statutory damages of $1,000 per negligent violation or $5,000 per intentional or reckless violation of the Act. There continues to be a flood of BIPA litigation, primarily against employers with biometric timekeeping/access systems that have failed to adequately notify and obtain written releases from their employees for such practices.

Biometric class action litigation has also been impacted by COVID-19. Screening programs in the workplace may involve the collection of biometric data, whether by a thermal scanner, facial recognition scanner or other similar technology. In late 2020, plaintiffs' lawyers filed a class action lawsuit on behalf of employees concerning their employer's COVID-19 screening program, which is alleged to have violated the BIPA. According to the complaint, employees were required to undergo facial geometry scans and temperature scans before entering company warehouses, without prior consent from employees as required by law. This case is still alive and well, at the start of 2022, after significant attempts by the defense, a federal district judge in Illinois declined to dismiss the proposed class action, as the allegations relating to violations regarding "possession" and "collection" of biometric data pass muster at this stage. Many businesses have been sued under the BIPA for similar COVID related claims in the past year, and 2022 will likely see continued class action litigation in this space.

In 2021, biometric technology-related laws began to evolve at a rapid pace, signaling a continued trend into 2022. In July 2021, New York City established BIPA-like requirements for retail and hospitality businesses that collect and use "biometric

identifier information" from customers. In September 2021, the City of Baltimore officially banned private use of facial recognition technology. Baltimore's local ordinance prohibiting persons (including residents, businesses, and most of the city government) from "obtaining, retaining, accessing, or using certain face surveillance technology or any information obtained from certain face surveillance technology". Other localities have also established prohibitions on use of biometric technology including Portland (Oregon), San Francisco. State legislatures have also increased focus on biometric technology regulation. In addition to Illinois's BIPA, Washington and Texas have similar laws, and states including Arizona, Florida, Idaho, Massachusetts and New York have also proposed such legislation. The proposed biometric law in New York state would mirror Illinois' BIPA, including its private right of action provision. In California, the CCPA also broadly defines biometric information as one of the categories of personal information protected by the law.

Additionally, states are increasingly amending their breach notification laws to add biometric information to the categories of personal information that require notification, including 2021 amendment in Connecticut and 2020 amendments in California, D.C., and Vermont. Similar proposals across the U.S. are likely in 2022.

In response to the constantly evolving legislation related to biometric technology, we have created an interactive biometric law state map to help businesses that want to deploy these technologies, which inevitably require the collection, storage, and/or disclosure of biometric information, track their privacy and security compliance obligations.

3. Ransomware Attacks

Ransomware attacks continued to make headlines in 2021 impacting large organizations, including Colonial Pipeline, Steamship Authority of Massachusetts, the NBA, JBS Foods, the D.C. Metropolitan Police Department and many more. Ransomware attacks are nothing new, but they are increasing in severity. There has been an increase in frequency of attacks and higher ransomware payments, in large part due to increased remote work and the associated security challenges. The healthcare industry in particular has been substantially impacted by the onset of the COVID-19 pandemic - a recent study by Comparitech found that ransomware attacks on the healthcare industry has resulted in a financial loss of over $20 billion in impacted revenue, litigation and ransomware payments and growing.

In fact, the FBI jointly with the Cybersecurity and Infrastructure Security Agency (CISA) went so far as to issue a warning to be on high alert for ransomware attacks for holidays in light of numerous targeted attacks over other holidays earlier in the year.

Moreover in 2021, the National Institute of Standards Technology (NIST) released a preliminary draft of its Cybersecurity Framework Profile for Ransomware Risk Management. The NIST framework provides steps for protecting against ransomware

attacks, recovering from ransomware attacks, and determining you organization's state of readiness to prevent and mitigate ransomware attacks.

Ransomware continues to present a significant threat to organizations as we move into 2022. Organizations may not be able to prevent all attacks, but it is important to remain vigilant and be aware of emerging trends.

Here are some helpful resources for ransomware attack prevention and response:

- **New Ransomware Tactics and Strains Emerge, Including Public Auctions of Stolen Data**
- **Small Michigan Medical Practice To Close Following Ransomware Attack**
- **3 Essential Steps For Responding To Ransomware Attacks**
- **Ransomware Attacks Prevention and Preparedness**

4. Biden Administration Prioritizes Cybersecurity

In large part due to significant threat of ransomware attacks discussed above, the Biden Administration has made clear that cybersecurity protections are a priority. In May of 2021, on the heels of the Colonial Pipeline ransomware attack that snarled the flow of gas on the east coast for days, the Biden Administration issued an Executive Order on "Improving the Nation's Cybersecurity" (EO). The EO was in the works prior to the Colonial Pipeline cyberattack, however was certainly prioritized as a result. The EO made a clear statement on the policy of the Administration, *"It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order."* This EO will mostly impacts the federal government and its agencies. However, several of the requirements in the EO will reach certain federal contractors, and also will influence the private sector.

Shortly after the Biden Administration issued the EO, it followed in August 2021 with the issuance of a National Security Memo (NSM) with the intent of improving cybersecurity for critical infrastructure systems. This NSM established an Industrial Control Systems Cybersecurity Initiative (the "Initiative") that will be a voluntary, collaborative effort between the federal government and members of the critical infrastructure community aimed at improving voluntary cybersecurity standards for companies that provide critical services.

The primary objective of the Initiative is to encourage, develop, and enable deployment of a baseline of security practices, technologies and systems that can provide threat visibility, indications, detection, and warnings that facilitate response capabilities in the

event of a cybersecurity threat. According to the President's Memo, "we cannot address threats we cannot see."

And most recently, in early January 2022, President Biden issued an additional NSM to improve the cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. "*Cybersecurity is a national security and economic security imperative for the Biden Administration, and we are prioritizing and elevating cybersecurity like never before…Modernizing our cybersecurity defenses and protecting all federal networks is a priority for the Biden Administration, and this National Security Memorandum raises the bar for the cybersecurity of our most sensitive systems,"* stated the White House in its issuance of the latest NSM.

The U.S. government will continue to ramp up efforts to strengthen its cybersecurity as we head into 2022, impacting both the public and private sector. Businesses across all sectors should be evaluating their data privacy and security threats and vulnerabilities and adopt measures to address their risk and improve compliance.

5. COVID-19 Privacy and Security Considerations

During 2020 and 2021, COVID-19 presented organizations large and small with new and unique data privacy and security considerations. And while we had high hopes that increased vaccination rates would put this pandemic in the rearview mirror, the latest omicron strand showed us otherwise. Most organizations, particularly in their capacity as employers, needed to adopt COVID-19 screening and testing measures resulting in the collection of medical and other personal information from employees and others. While the Supreme Court has stayed OSHA's ETS mandating that employers with 100+ employees require COVID-199 vaccination and the Biden Administration ultimately withdrew same, some localities have instituted mandates depending on industry, and many employers have voluntarily decided to institute vaccine requirements for employees. Ongoing vigilance will be needed to maintain the confidential and secure collection, storage, disclosure, and transmission of medical and COVID-19 related data that may now include tracking data related to vaccinations or the side effects of vaccines.

Several laws apply to data the organizations may collect in this instance. In the case of employees, for example, the Americans with Disability Act (ADA) requires maintaining the confidentiality of employee medical information and this may include COVID-19 related data. Several state laws also have safeguard requirements and other protections for such data that organization should be aware of when they or others on their behalf process that information.

Many employees will continue to telework during 2022 (and beyond). A remote workforce creates increased risks and vulnerabilities for employers in the form of sophisticated phishing email attacks or threat actors gaining unauthorized access through unsecured remote access tools. It also presents privacy challenges for organizations trying to balance business needs and productivity with expectations of

privacy. These risks and vulnerabilities can be addressed and remediated through periodic risk assessments, robust remote work and bring your own device policies, and routine monitoring.

As organizations continue to work to create safe environments for the in-person return of workers, customers, students, patients and visitors, they may rely on various technologies such as wearables, apps, devices, kiosks, and AI designed to support these efforts. These technologies must be reviewed for potential privacy and security issues and implemented in a manner that minimizes legal risk.

Some reminders and best practices when collecting and processing information referred to above and rolling out these technologies include:

- Complying with applicable data protection laws when data is collected, shared, secured and stored including the ADA, Genetic Information Nondiscrimination Act, CCPA, GDPR and various state laws. This includes providing required notice at collection under the California Consumer Privacy Act (CCPA), or required notice and a documented lawful basis for processing under the GDPR, if applicable.
- Complying with contractual agreements regarding data collection; and
- Contractually ensuring vendors who have has access to or collect data on behalf of the organization implement appropriate measures to safeguard the privacy and security of that data.

6. "New" EU Standard Contractual Clauses

In July of 2020 the Court of Justice of the European Union (CJUE) published its decision in *Schrems II* which declared the EU-US Privacy Shield invalid for cross border data transfers and affirmed the validity standard contractual clauses ("SCCs) as an adequate mechanism for transferring person data from the EEA, subject to heightened scrutiny. However, the original SCCs were unable to adequately address the EU Commission's concerns about the protection of personal data.

On June 4, 2021, the EU Commission adopted "new" modernized SCCs to replace the 2001, 2004, and 2010 versions in use up to that point - effective since September 27,2021. The EU Commission updated the SCCs to address more complex processing activities, the requirements of the GDPR, and the *Schrems II* decision. These clauses are modular so they can be tailored to the type of transfer. if a data exporter transfers data from the EU to a U.S. organization, the U.S. organization must execute the new SCCs unless the parties rely on an alternate transfer mechanism or an exception exists. This applies regardless of whether the U.S. company receives or accesses the data as a data controller or processor. The original SCCs apply to controller-controller and controller-processor transfers of personal data from the EU to countries without a Commission adequacy decision. The updated clauses are expanded to also include

processor-processor and processor-controller transfers. While the existing SCCs were designed for two parties, the new clauses can be executed by multiple parties. The clauses also include a "docking clause" so that new parties can be added to the SCCs throughout the life of the contract.

The obligations of the data importer are numerous and include, without limitation:

- documenting the processing activities it performs on the transferred data,
- notifying the data exporter if it is unable to comply with the SCCs,
- returning or securely destroying the transferred data at the end of the contract,
- applying additional safeguards to "sensitive data,"
- adhering to purpose limitation, accuracy, minimization, retention, and destruction requirements,
- notifying the exporter and data subject if it receives a legally binding request from a public authority to access the transferred data, if permitted, and
- challenging a public authority access request if it reasonably believes the request is unlawful.

The SCCs require the data exporter to warrant there is no reason to believe local laws will prevent the importer from complying with its obligations under the SCCs. In order to make this representation, both parties must conduct and document a risk assessment of the proposed transfer.

If an organization that transfers data cross border has not already done so it should be implementing the new procedures and documents for the SCCs. This is, of course, if they are not relying on an alternate transfer mechanism or an exception exists. Organizations will also need to review any ongoing transfers made in reliance on the old SCCs and take steps to comply. As with new transfers, this will require a documented risk assessment and a comprehensive understanding of the organization's process for accessing and transferring personal data protected under GDPR. For additional guidance on the new EU SCCs, our comprehensive FAQs are available here.

7. TCPA

In April 2021, the U.S. Supreme Court issued a monumental decision with significant impact on the future of Telephone Consumer Protection Act (TCPA) class action litigation. The court narrowly ruled to qualify as an "automatic telephone dialing system", a device must be able to either "store a telephone number using a random or sequential generator or to produce a telephone number using a random or sequential number generator". The underlying decision of the Ninth Circuit was reversed and remanding.

The Supreme Court unanimously concluded, in a decision written by Justice Sotomayor, that to qualify as an "automatic telephone dialing system" under the TCPA, a device

must have the capacity either to store, or to produce, a telephone number using a random or sequential number generator.

"Expanding the definition of an autodialer to encompass any equipment that merely stores and dials telephone numbers would take a chainsaw to these nuanced problems when Congress meant to use a scalpel," Justice Sotomayor pointed out in rejecting the Ninth Circuit's broad interpretation of the law.

Moreover, Sotomayor noted that, "[t]he statutory context confirms that the autodialer definition excludes equipment that does not "us[e] a random or sequential number generator."" The TCPA's restrictions on the use of autodialers include, using an autodialer to call certain "emergency telephone lines" and lines "for which the called party is charged for the call". The TCPA also prohibits the use of an autodialer "in such a way that two or more telephone lines of a multiline business are engaged simultaneously." The Court narrowly concluded that "these prohibitions target a unique type of telemarketing equipment that risks dialing emergency lines randomly or tying up all the sequentially numbered lines at a single entity."

The Supreme Court's decision resolved a growing circuit split, where several circuits had previously interpreted the definition of an ATDS broadly to encompass any equipment that merely stores and dials telephone numbers, while other circuits provided a narrower interpretation, in line with the Supreme Court's ruling. It was expected the Supreme Court's decision would help resolve the ATDS circuit split and provide greater clarity and certainty for parties facing TCPA litigation. In the six months following the Supreme Court's decision, the Institute of Legal Reform documented a 31% drop in TCPA filings, compared to the six months prior to the ruling. Nonetheless, many claims based on broad ATDS definitions are still surviving early stages of litigation in the lower courts, and some states have enacting (or are considering) "mini-TCPAs" which include a broader definition of ATDS. While the Supreme Court's decision was considered a win for defendants facing TCPA litigation, organizations are advised to review and update their telemarketing and/or automatic dialing practices to ensure TCPA compliance, as they move into 2022.

8. Global Landscape of Data Privacy & Cybersecurity

2021 was a significant year for the global landscape of data privacy and security. As discussed above, on June 4th, the European Commission adopted new standard contractual clauses for the transfer of personal data from the EU to "third countries", including the U.S. On August 20, China passed its first comprehensive privacy law, the Personal Information Protection Law (PIPL), similar in kind to the EU's GDPR. The law took effect in November of 2021. In addition, China published 1) Security Protection Regulations on the Critical Information Infrastructure and 2) the Data Security Law which aims to regulate data activities, implement effective data safeguards, protect individual and entity legitimate rights and interests, and ensure state security – both effective September of 2021. Finally, Brazil enacted Lei Geral de Proteção de Dados

Pessoais (LGPD), its first comprehensive data protection regulation, again with GDPR-like principles. The LGPD became enforceable in August of 2021.

In 2022, U.S. organizations may face increased data protection obligations as a result of where they have offices, facilities, or employees; whose data they collect; where the data is stored; whether it is received from outside the U.S.; and how it is processed or shared. These factors may trigger country-specific data protection obligations such as notice and consent requirements, vendor contractual obligations, data localization or storage concerns, and safeguarding requirements. Some of these laws may apply to data collection activities in a country regardless of whether the U.S. business is located there.

9. Federal Consumer Privacy Law

Numerous comprehensive data protection laws were proposed at the federal level in recent years. These laws have generally stalled due to bipartisan debate over federal preemption and a private right of action. And while, every year, we ask ourselves whether this will be the year, 2022 may indeed be the year the U.S. enacts federal consumer privacy law. 2022 has barely begun and a coalition which includes the U.S. Chamber of Congress together with local business organizations in over 20 states have issued a letter to Congress highlighting the importance of enacting a federal consumer privacy law as soon as possible.

"Data is foundational to America's economic growth and keeping society safe, healthy and inclusive…Fundamental to the use of data is trust," the coalition noted. "A national privacy law that is clear and fair to business and empowering to consumers will foster the digital ecosystem necessary for America to compete."

Moreover, with California, Virginia, and Colorado all with comprehensive consumer privacy laws (as discussed above), and approximately half of U.S. states contemplating similar legislation, there is a growing patchwork of state laws that "threatens innovation and create consumer and business confusion," as stated in the coalition's letter to Congress.

Will 2022 be the year the U.S. government enacts a federal consumer privacy law? Only time will tell. We will continue to update as developments unfold.

10. Cyber Insurance

Over the past several years, if your organization experienced a cyberattack, such as ransomware or a diversion of funds due to a business email compromise (BEC), and you had cyber insurance, you likely were very thankful. However, if you are renewing that policy (or in the cyber insurance market for the first time), you are probably looking at much steeper rates, higher deductibles, and even co-insurance, compared to just a year or two ago. This is dependent on finding a carrier to provide competitive terms, although there are some steps organizations can take to improve insurability.

Claims paid under cyber insurance policies are significantly up, according to Marc Schein*, CIC, CLCS, National Co-Chair Cyber Center of Excellence for Marsh McLennan Agency who closely tracks cyber insurance trends. Mr. Schein identified the key drivers hardening the cyber insurance market: ransomware and business interruption.

According to Fitch Ratings' Cyber Report 2020, insurance direct written premiums for the property and casualty industry increased 22% in the past year to over $2.7 billion, representing the demand for cyber coverage. The industry statutory direct loss plus defense and cost containment (DCC) ratio for standalone cyber insurance rose sharply in 2020 to 73% compared with an average of 42% for the previous five years (2015-2019). The average paid loss for a closed standalone cyber claim moved to $358,000 in 2020 from $145,000 in 2019.

The effects of these, other increases in claims, and losses from cyberattacks had a dramatic impact on cyber insurance. Perhaps the most concerning development for organizations in the cyber insurance market is the significantly increased scrutiny carriers are applying to an applicant's insurability.

There are no silver bullets, but implementing administrative, physical and technical safeguards to protect personal information may dramatically reduce the chances of a cyberattack, and that is music to an underwriter's ears. As an organization heads into 2022, ensuring such safeguards are instituted and regularly reviewed, can go a long way.

* * * * *

For these reasons and others, we believe 2022 will be a significant year for privacy and data security.