By Alex Nisenbaum

Recent Trends in U.S. State Data Privacy and Security Law

The United States has seen significant new data privacy and security legislation in recent years at the state level, while federal efforts to enact such legislation have stalled. Two broad state legislative trends have taken hold in recent years. First, three states have passed comprehensive data privacy laws, and legislatures in many more states have introduced such laws for consideration. For states that have not passed these laws in recent legislative sessions, it is widely expected that the same or similar proposals will be introduced in upcoming sessions. Second, several states have passed data security legislation mandating compliance with industry accepted information security standards or incentivizing implementation of specific safeguards that broadly track requirements of such standards, indicating a growing consensus among regulators regarding the standard of care for data protection. This paper describes enforcement trends relating to the California Consumer Privacy Act (CCPA), the first comprehensive privacy law in the United States, and the similarities and differences between state privacy and security legislation that companies will need to navigate to comply with numerous state laws and regulations that have either recently become effective or will become effective in the next twelve to eighteen months.

▪ **Alex Nisenbaum** of Blank Rome LLP advises clients on data privacy and information security laws and regulations, including compliance with HIPAA/HITECH; the Gramm-Leach-Bliley Act; the California Consumer Privacy Act; cross-border data transfer; and state privacy, data protection and breach notification requirements. Alex synthesizes the patchwork of state and federal legal requirements to assist clients in bringing innovative products to market and operationalize compliance programs that are in line with their business goals. He is certified as an information privacy professional by the International Association of Privacy Professionals.

State Omnibus Privacy Laws

California Consumer Privacy Act Enforcement Trends

The California legislature hastily passed the CCPA in June of 2018 to prevent a more stringent ballot initiative authored by privacy activist Alastair Mactaggart from being presented directly to California voters. The CCPA provides California consumers (i.e., California residents) a number of rights with respect to their personal information, such as the right to know what information has been collected by a business, the right to delete personal information, and the right to opt-out of the "sale" of personal information. The CCPA also includes strict notice requirements for businesses, and obligations for contracting with service providers, among other requirements, and provides consumers with a private right of action in the event a data breach occurs as a result of a business's failure to use reasonable security. The CCPA's regulatory framework is far-reaching in part because the definition of personal information is incredibly broad – "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Many components of the CCPA, including the broad definition of regulated personal information, have become models for omnibus privacy legislation in other states.

Enforcement of the CCPA began on July 1, 2020. On July 19, 2021, the California Attorney General issued a press release summarizing its first year of CCPA enforcement actions and released brief summaries of twenty-seven exemplary enforcement cases. The Attorney General reported that 75% of businesses that received a notice of an alleged violation since the Attorney General began enforcing the CCPA on July 1, 2020, had taken action to come into compliance within the 30-day statutory cure period. The remaining 25% were currently within their thirty-day window for cure or under active investigation. The enforcement action summaries provide lessons on key areas of scrutiny by the Attorney General.

Companies should note that the summaries show that enforcement has been undertaken against companies in a diverse set of industries. Accordingly, businesses should not assume that their CCPA compliance practices will not be scrutinized based on the industry in which they operate.

The CCPA enforcement case examples do not include all of the details of specific violations or curative actions that were taken and deemed sufficient by the California Attorney General, but several themes emerge in the summaries. Many of the enforcement cases address deficiencies in notices to consumers such as failing to include a description of consumer rights or request submission methods, or a notice of financial incentive. Inadequate or missing "Do Not Sell My Personal Information" links were also cited in several cases, providing some additional clarity on the Attorney's position that data collection by a third party via cookies is a sale unless the business obtains appropriate contractual commitments from the third party to make them a "service provider" under the CCPA.

> Failure to timely respond to consumer rights requests and noncompliant service provider contracts were additionally cited.

These are all areas of relatively low-hanging fruit for enforcement. It is easy for the Attorney General to review a company's website and privacy notice to see whether disclosures are deficient and whether the company has not provided a "Do Not Sell My Personal Information" link. Companies are well advised to ensure that these outward facing signs of compliance are complete as well as to ensure appropriate documentation is available to back up compliance decisions, such as contracts with all service providers, including digital advertising and website analytics service providers, that include language mandated by the CCPA restricting service provider use of personal information.

California Privacy Rights Act

Shortly after enforcement of the CCPA began, Alastair Mactaggart announced that he formally filed an initiative to appear on the November 2020 ballot. The initiative put the California Privacy Rights Act (CPRA) before California voters. Subject to limited exemptions for certain types of personal information, an entity is subject to the CPRA if it is for-profit, does business in California, alone or jointly with others determines the purposes and means of processing personal information and: (a) has gross annual revenue in excess of $25 million; (b) alone or in combination, annually buys, sells or shares the personal information of 100,000 or more consumers or households; or (c) derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

The CPRA easily passed and provides for sweeping amendments to the CCPA. The CPRA will be effective January 1, 2023, and will, among other things:

- provide consumers with a right to limit the use and disclosure of "sensitive personal information" (e.g., financial and health information, racial or ethnic origin, sexual orientation, and precise geolocation);
- triple the CCPA's fines for violating the law governing the collection and sale of children's personal information;
- create a new right to correct inaccurate personal information;
- expand the right to opt-out to include the right to opt out of the "sharing" of personal information for cross-context behavioral advertising;
- significantly expand requirements for contracting with vendors that process personal information on behalf of a business (including parties that qualify as "service providers" and parties that qualify as newly "contractors);
- remove the thirty-day cure period provided for under the CCPA; and
- establish the California Privacy Protection Agency, which would implement and enforce the CCPA through administrative action, including audits and fines, while leaving civil enforcement to the Attorney General.

Virginia Consumer Data Protection Act

Virginia was the second state to pass comprehensive privacy legislation. Entities are subject to the Virginia Consumer Data Protection Act (VCDPA) if they conduct business in the Commonwealth or produce products or services that target residents of the Commonwealth, and: (a) during a calendar year, control, or process personal data of at least 100,000 consumers; or (b) control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data. The VCDPA defines "personal data" broadly, similar to the CCPA. A "consumer" is an individual who is a Virginia resident acting only in an individual or household context. Individuals acting in a commercial or employment context, job applicants and beneficiaries of individuals acting in an employment context do not qualify as consumers under the VCDPA. Unless the California legislature takes action to extend a partial exemption from the CCPA for employment-related personal information to continue after January 1, 2023, this will represent a major difference in application of the California and Virginia laws.

Government agencies and authorities, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), "covered entities" or "business associates" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), nonprofit organizations and institutions of higher education are exempt from the VCDPA. Under the CPRA, data subject to certain laws such as the GLBA, HIPAA and other laws is exempt, but the entity regulated by those laws may still be covered with respect to other personal information that it collects.

The VCDPA borrows "controller" and "processor" concepts from the EU's General Data Protection Regulation (GDPR) rather than the "business" and "service provider" terms used by the CCPA. Most of the VCDPA's obligations fall on controllers. However, certain obligations are directly applicable to processors. Additionally, the VCDPA mimics the requirements of Article 28 of the GDPR by requiring nearly identical provisions to those required by the GDPR be included in contracts between controllers and processors.

Similar to the CCPA, the VCDPA requires controllers to adhere to transparency principles when processing personal data by making a privacy notice reasonably accessible to consumers. The VCDPA does not provide instruction about what is "reasonably accessible," so an entity may wish to consider how they normally interact with Virginia residents in determining how the entity provides notice (e.g., whether a physical or verbal notice may be appropriate) in addition to providing a notice via any public facing website the entity may maintain.

The VCDPA provides Virginians with similar rights to those afforded by the CPRA. The VCDPA provides consumers the rights to know whether a company is processing the consumer's personal data and access their personal data if it is being processed; correct inaccuracies; delete their personal data; obtain a copy of their data; and opt out of targeted advertising, the sale of personal data and certain profiling.

The definition of "sale' is narrower than the CCPA definition. By requiring actual monetary consideration, the VCPDA is more aligned with the Colorado approach to sweep up pure data broking activities. Where the CCPA approach was to define "sale" broadly enough to encompass sharing data through cookies for targeted advertising and website analytics purposes (at least in the California Attorney General's view), the VCDPA takes a more direct route by providing a specific right to opt out of targeted advertising. The VCDPA also provides the right to opt out of profiling that is used to make decisions that produce legal or similarly significant effects concerning the consumer. What decisions may produce effects "similarly significant" to legal effects is not defined, meaning companies will need to carefully evaluate any profiling activities they undertake to determine whether a consumer may opt out.

Timeframes for responses to consumer rights requests are consistent with the CPRA and the VCDPA is less prescriptive about the methods that must be provided to consumers to submit requests and how companies should authenticate those requests. Interestingly, the VCDPA requires companies to establish and make conspicuously available an appeal process where a consumer may appeal a company's initial decision with respect to any rights request. If the appeal is denied, the company must provide the consumer with directions about how to contact the Virginia Attorney General and submit a complaint. This could prove to be a significant way for perceived issues to come to the attention of the Attorney General's office.

The VCDPA prohibits the processing of sensitive data without obtaining the consumer's consent. This differs from the CPRA, which provides consumers the ability only to limit the processing of sensitive personal information.

In contrast to the CPRA, the VCDPA requires entities undertake data protection assessments in a number of specific instances, such as targeted advertising, the sale of personal data, processing of sensitive data, specific instances involving profiling and where such processing poses a heightened risk of harm to consumers. The CPRA defers specific rules around conducting risk assessments to the administrative rulemaking process. The Virginia Attorney General is able to obtain completed risk assessments pursuant to an investigative demand, potentially giving it significant insight into a company's processing activities and compliance processes.

Under the VCDPA, the Virginia Attorney General has exclusive enforcement authority. The VCDPA requires the Attorney General to provide a 30-day cure period and bars Attorney General action if a business successfully cures its violation. The Virginia Attorney General may recover a civil penalty of up to $7,500 per violation plus reasonable expenses incurred in investigating and preparing the case, including attorneys' fees. The VCDPA does not require any implementing regulations.

Colorado Privacy Act

Following California and Virginia, Colorado was the third state to enact comprehensive privacy legislation. The Colorado Privacy Act (Colo PA), which was passed on June 8, 2021, provides data privacy rights for Colorado residents (i.e., "consumers") similar to those provided under the CCPA

and VCDPA. The Colo PA applies to entities that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to Colorado residents and: (a) controls or processes the personal data of 100,000 consumers or more during a calendar year; or (b) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.

The Colo PA protects "personal data," which is broadly defined as information that is linked or reasonably linkable to an identified or identifiable individual. Personal data does not include de-identified data or publicly available information. Like the VCDPA, individuals acting in a commercial or employment context, job applicants and beneficiaries of individuals acting in an employment context do not qualify as consumers under the Colo PA.

Additionally, similar to the CPRA and VCDPA, the Colo PA exempts several entities and types of personal information governed under federal law, including protected health information and de-identified information under HIPAA, financial institutions and nonpublic personal information under the GLBA, and information regulated by the Fair Credit Reporting Act, Children's Online Privacy Protection Act of 1998, Family Educational Rights and Privacy Act of 1974, and the Driver's Privacy Protection Act of 1994.

Like the GDPR and VCDPA, the Colo PA distinguishes between controllers and processors. The obligation of a business under the law depends upon the role of the business with respect to the personal data at issue. Controllers bear most responsibilities under the Colo PA. However, processors have direct obligations to assist controllers with their compliance efforts.

Like the VCDPA, controllers and processors are required under the Colo PA to enter into a written contract which emulates the requirements under Article 28 of the GDPR. For instance, the agreement must set forth the type of personal data subject to the processing and the nature, the purpose and duration of the processing, only allow the processor to engage a subcontractor after the processor provides the controller an opportunity to object, and require the processor to flow down compliance obligations under the Colo PA to subcontractors by written agreement.

The Colo PA provides consumers the right to opt out of the processing of their personal data for targeted advertising, opt out of the sale of their personal data (broadly defined as the exchange of personal data for monetary or other valuable consideration by a controller to a third party), and processing of personal data for profiling that produces legal or similarly significant effects concerning a consumer. The Colo PA also provides consumers rights to access, obtain a portable copy of, correct, and delete their personal data. Consistent with the approach of other state laws, the Colo PA requires controllers to provide a privacy notice to consumers.

With respect to the right to opt out, effective July 1, 2024, consumers must be able to exercise their opt-out right through a user-selected universal opt-out mechanism that meets technical specifications to be established by the Colorado Attorney General. The Colorado Attorney General will establish the technical specifications by July 1, 2023. The California Attorney General recently announced that businesses must honor the global privacy control by treating it as an opt out. If the Colorado Attorney General adopts different technical specifications, it will create complexities in compliance processes for entities subject to the various comprehensive state privacy laws.

The Colo PA prohibits process sensitive data without consumer consent – the same approach as the VCDPA. Consent cannot be obtained by way of acceptance of general or broad terms of use or through "dark patterns."

Controllers are required to conduct and document a data protection assessment of each of its processing activities that present a heightened risk of harm to a consumer. Processing that presents a heightened risk of harm to a consumer includes processing sensitive data, processing for purposes of targeted advertising, and selling personal data or profiling if there is a reasonably foreseeable risk of financial or physical injury to consumers, among other activities. The Colo PA's examples of processing that presents a heightened risk of harm is not exclusive and so controllers will need to initially evaluate all processing activities to determine whether they potentially fall into this category and require an assessment. Controllers must make the data protection assessments available to the Colorado Attorney General upon request.

The Colo PA is enforced by the Colorado Attorney General and district attorneys and does not provide a private right of action. A 60-day cure period to rectify non-compliance is provided before the Colorado Attorney General or district attorney may take enforcement action. However, this cure period will only be provided until January 1, 2025. Non-compliance with the Colo PA can result in civil penalties of up to $20,000 for each violation up to a total of $500,000 for any related series of violations.

Data Breach 2.0

In another trend, states have recently passed or amended existing data breach notification statutes to strengthen information security requirements with respect to personal data. At least four states have amended their data breach notification statutes in recent years to add security requirements or incentivize alignment with industry accepted information security standards. These new laws reflect a growing consensus among state law and regulators regarding the standard of care for cybersecurity.

Security Mandates

The New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) is the most comprehensive and prescriptive recent example of state data security regulation. Passed in July 2019, the SHIELD Act follows the example of the Massachusetts regulations on the Standards for the protection of personal information of residents of the Commonwealth (Massachusetts Cyber Regulations). The SHIELD Act amended New York's data breach notification law to broaden notification obligations and impose new data security requirements on companies to secure "private information," which is defined as any information that can be used to identify a natural person in combination with

a social security number, driver's license or other identification card number, account number, credit or debit card number in combination with information that would provide access to an individual's account, biometric information and use credentials permitting access to an online account. The heightened data security requirements took effect on March 21, 2020.

The SHIELD Act was not the first data security law enacted in New York. Three years earlier, the state adopted the New York Department of Financial Services (NYDFS) Cybersecurity Regulations, which established heightened security requirements for covered financial entities. However, unlike the NYDFS Cybersecurity Regulations, and consistent with the Massachusetts Cyber Regulations, the SHIELD Act broadly covers all businesses that store information of New York residents, regardless of industry.

The SHIELD Act requires businesses to implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information. Entities that are subject to, and in compliance with, laws like HIPAA, GLBA or the NYDFS Cybersecurity Regulations, are deemed to be compliant with SHIELD Act requirements. All other businesses must implement a data security program that includes reasonable administrative, physical, and technical safeguards. Businesses can maintain compliance with such security requirement by maintaining the following administrative, physical, and technical safeguards:

- Reasonable Administrative Safeguards
  - o designate an employee who coordinates the security program
  - o perform assessments that identify reasonably foreseeable external and internal risks
  - o assess the sufficiency of safeguards in place to control identified risks
  - o provide reasonable training and management of employees in the security program practices and procedures
  - o establish procedures to select service providers capable of maintaining appropriate safeguards, and require that the service providers implement those safeguards by contract
  - o ensure procedures adjust to reflect business changes and new circumstances
- Reasonable Technical Safeguards
  - o assess risks in network and software design
  - o assess risks in information processing, transmission, and storage
  - o detect, prevent, and respond to attacks or system failures
  - o regularly test and monitor the effectiveness of key controls, systems, and procedures
- Reasonable Physical Safeguards
  - o assess risks of information storage and disposal
  - o detect, prevent, and respond to intrusions
  - o protect against unauthorized access to, or use of, private information during or after the collection, transportation and destruction or disposal of the information
  - o properly delete private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Small businesses are not exempt from the SHIELD Act, but they are not held to the prescriptive standards for safeguards with respect to what constitutes a reasonable security program. Instead, a small business must have reasonable administrative, technical, and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of its activities, and the sensitivity of the private information collected.

The California, Virginia, and Colorado omnibus privacy statutes also place an emphasis on the security of personal information and in several respects require the same sorts of safeguards, such as performing risk assessments and managing third-party vendors. Accordingly, by implementing certain industry standard information security safeguards, companies can leverage these compliance processes and procedures across a number of jurisdictions.

While the SHIELD Act does not create a private right of action, the SHIELD Act makes any violation of the data security requirements a violation of New York General Business Law § 349, which prohibits deceptive acts and practices in the conduct of any business. These violations are enforceable by the New York Attorney General, with civil penalties of $5,000 per violation.

Safe Harbor Approach

In contrast to establishing detailed, prescriptive standards for security and making violations a fineable offense, Ohio, Utah, and Connecticut are examples of states that have used a safe harbor approach to incentivize companies to adopt appropriate cybersecurity protections.

Ohio

The Ohio Data Protection Act (Ohio DPA) provides companies with a safe harbor against data breach claims sounding in tort (such as negligence) brought under the laws or in the courts of Ohio for companies that implement, maintain, and comply with one of several industry-recognized cybersecurity programs. The Ohio DPA expressly provides that the act does not "create a minimum cybersecurity standard that must be achieved" or "impose liability upon businesses that do not obtain or maintain practices in compliance with the act."

To qualify for the safe harbor, an entity must implement a written cybersecurity program designed to: (a) protect the security and confidentiality of personal information; (b) protect against anticipated threats or hazards to the security or integrity of personal information; and (c) protect against unauthorized access to and acquisition of personal information that is likely to result in a material risk of identity theft or fraud. The act provides that the scale and scope of the company's cybersecurity program should be consummate with the company's size and complexity; the nature and scope of its activities; the sensitivity of the personal information maintained by the company; the cost and availability of tools to improve information security; and the resources available to the company.

In addition, the act also requires the entity's cybersecurity program to "reasonably conform" to one of the following cybersecurity frameworks:

- National Institute of Standards and Technology's (NIST) Cybersecurity Framework
- NIST Special Publication 800-171 or Special Publications 800-53 and 800-53a
- Federal Risk and Authorization Management Program's (FedRAMP) Security Assessment Framework
- Center for Internet Security's Critical Security Controls for Effective Cyber Defense
- International Organization for Standardization (ISO)/International Electrotechnical Commission's (IEC) 27000 series of information security standards.

For businesses that accept payment cards, the Ohio DPA requires that the businesses' cybersecurity programs must also comply with the Payment Card Industry Data Security Standard (PCI-DSS), in addition to one of the generally applicable frameworks identified above, to qualify for the affirmative defense. Similarly, companies subject to certain state or federally mandated sector-specific laws may rely on the affirmative defense if, in addition to conforming with one of the above generally applicable frameworks, they can establish that their plan conforms to any additional security requirements, such as the security requirements identified in HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH), the GLBA or the Federal Information Security Modernization Act.

Utah

Utah's Cybersecurity Affirmative Defense Act (CADA) provides companies that meet the law's written cybersecurity program requirements with an affirmative defense to claims that are brought under the laws of Utah or in Utah courts alleging a failure to implement reasonable security controls that resulted in a security incident, failure to appropriately respond to a security incident, or failure to appropriately notify individuals whose personal information was compromised in a security incident.

Like the Ohio DPA, CADA requires a company to implement a written cybersecurity program that "reasonably conforms" to one of several recognized cybersecurity frameworks to qualify for the affirmative defense. The approved cybersecurity frameworks are NIST Special Publication 800-171, NIST Special Publications 800-53 and 800-53a, the FedRAMP Security Assessment Framework, the Center for Internet Security Critical Security Controls for Effective Cyber Defense, and the ISO/IEC 27000 series of information security standards.

Alternatively, companies can satisfy this requirement by implementing a "reasonable security program," which is defined under the CADA as a program that, among other things: (a) designates an employee to oversee and facilitate the program; (b) utilizes practices and procedures to detect, prevent and respond to security incidents; (c) provides training to employees on the company's data security practices; and (d) utilizes risk assessments to test and monitor its data security practices. In addition, a company's cybersecurity program must be of an appropriate scale and scope, taking into account factors similar to those listed by the Ohio DPA.

A company is precluded from claiming the affirmative defense if it had actual notice of a threat to the security of personal information, did not act in a reasonable amount of time to remediate and neutralize the threat, and the threat resulted in a security incident.

Connecticut

The Connecticut Legislature passed HB 6607 in early June 2021 to amend its data breach notification law to create a limited safe harbor for entities impacted by a data breach. HB 6607 prohibits courts from assessing punitive damages for tort claims against an entity that experiences a data breach if the entity has created, maintained and complied with a written cybersecurity program protecting restricted information that conforms to an industry-recognized framework such as NIST Special Publication 800-171, NIST Special Publications 800-53 and 800-53a, the FedRAMP Security Assessment Framework, the Center for Internet Security Critical Security Controls for Effective Cyber Defense, the ISO/IEC 27000 series of information security standards and/or federal laws such as HIPAA, GLBA, and, if the entity processes payment card data, PCI-DSS.

Similar to the Ohio DPA and CADA, HB 6607 requires that the scale and scope of a company's cybersecurity program should take into account the company's size and complexity, the nature and scope of its activities, the sensitivity of the personal information maintained by the company, the cost and availability of tools to improve information security, and the resources available to the company.

Federal Efforts

At least twenty-four privacy related bills have been introduced in the 117th Congress. These proposals range from attempts at comprehensive federal privacy legislation to more targeted legislation addressing topics such as children's privacy, use of COVID-19-related health information, social media platforms, and use of biometric surveillance by the federal government. However, there is a lack of consensus about whether similar federal legislation should include a private right of action or, even if no private right of action is included, which governmental agency should be tasked with enforcing the legislation. There is also a lack of consensus at the federal level, generally across party lines, regarding whether and to the extent federal legislation should preempt state privacy laws. So, while this area continues to attract proposals on both sides of the aisle, there are no significant proposals that currently appear likely to pass this year and these issues will certainly need to be resolved to advance any federal legislation.

Key Takeaways

Over thirty states have introduced some form of comprehensive privacy bill in the three years since the passage of the CCPA. Washington, Oklahoma, Florida, New York, Pennsylvania, and Ohio are jurisdictions that have had proposed bills make some headway through the legislative process, with Washington and Florida, among other states, nearly passing proposed laws in recent legislative sessions.

In general, these proposals provide for principles and rights that are similar to the California, Virginia, and Colorado approaches. Many legislative proposals have included some type of private right of action, though at the state level the enforcement mechanism continues to be a significant point of contention, with a private right of action viewed as too costly by the business community and exclusive attorney general enforcement seen as not effective enough for consumers by consumer privacy advocates. Expect to see continued efforts on the state level in the new year as legislative sessions begin again and state legislatures pick up prior proposals and consider new ones. Unless and until the federal government passes preemptive legislation, the complex patchwork of state data privacy and security laws promises to continue to grow and create compliance challenges for national businesses.

To develop an agile data privacy and security compliance program that can evolve with the changing legal landscape, companies should invest in a robust data inventory initiative to ensure a solid understanding of the types of personal data processed by the company, where the data is located, the business purposes for which it is used, and with whom the personal data is shared. This will allow for the design and implementation of efficient, scalable processes to respond to consumer rights requests, help inform the prioritized deployment of safeguards to protect the data and facilitate accurate and comprehensive notices to individuals, assessments, and other processes that comply with the myriad applicable requirements.