edgile

GRC REPORT

GOVERNANCE, RISK MANAGEMENT, COMPLIANCE

The 2019 Compliance Landscape Report

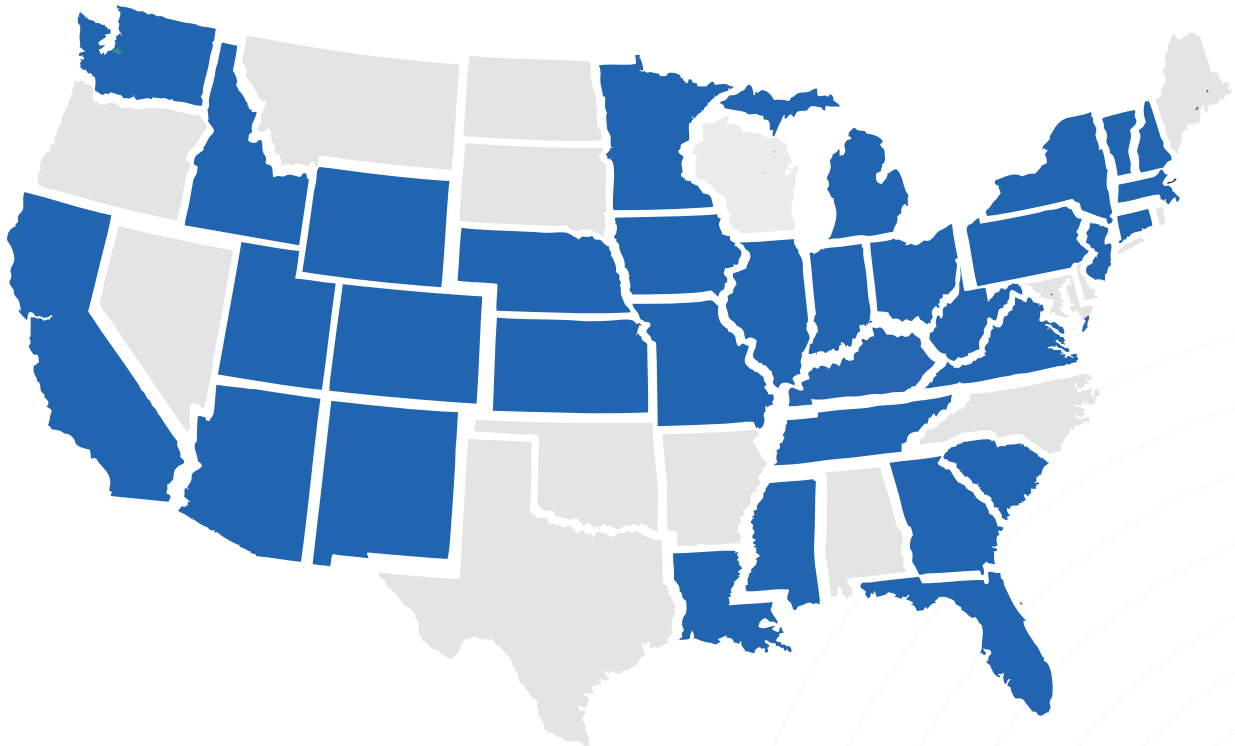
EDGILE.COM

States Continue to Drive the Cyber Regulatory Train as Push to Establish a National Privacy Standard Gains Momentum

As initially reported by Edgile in 2018, states continued to take the lead in implementing and enforcing regulatory initiatives in the areas of consumer information privacy and data security. This is creating momentum that has begun to translate into movements toward federal privacy rule discussions in 2019 and beyond.

State Legislative and Enforcement Activity

In 2018, at least **35 states** (in addition to the District of Columbia and Puerto Rico) considered more than 265 bills and resolutions pertaining to cybersecurity. **Approximately 50 of these measures became law.**



2018 Cybersecurity Legislation

California

CA A 1678, Chap. 2018-96
Requires the Secretary of State to adopt regulations describing best practices for storage and security of voter registration information received by an applicant. Requires a person or entity who has received voter registration information pursuant to an application to disclose a breach in the security of the storage of the information to the Secretary of State. Makes it a misdemeanor to distribute misleading or false information to a voter.

CA A 1859, Chap. 2018-532
Requires a consumer credit reporting agency that owns, licenses, or maintains personal information about a state resident, or an entity that has a contract with a consumer credit reporting agency and maintains personal information on behalf of a reporting agency that poses a significant risk to a breach in the system, to take certain measures to protect that data. Provides for civil action to recover damages, civil penalties, and attorney's fees.

CA A 1906, Chap. 2018-860
Requires a manufacturer that sells or offers to sell a connected device in California to equip the connected device with a reasonable security feature or features appropriate to the nature and function of the device that is designed to protect the device from unauthorized remote access or use. Provide that equipping a connected device with a means for authentication outside a local area network is deemed a reasonable security feature if it meets certain requirements.

CA A 2225, Chap. 2018-535
Requires the Secretary of State, in consultation with the Department of Technology, to approve and adopt appropriate uniform statewide standards for the purpose of storing and recording permanent and nonpermanent documents in electronic media. Requires that cloud computing to be defined by the Department of Technology based on industry-recognized standards. Imposes certain requirements on a cloud computing storage service used by agencies.

CA A 2813, Chap. 2018-768
Establishes in statute the California Cybersecurity Integration Center within the Office of Emergency Services to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in the state.

CA A 3075, Chap. 2018-241
Creates within the Secretary of State the Office of Elections Cybersecurity to coordinate efforts between the Secretary of State and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections in the state.

CA S 327, Chap. 2018-886
Requires a manufacturer of a connected device to equip such device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

CA S 532, Chap. 2018-557
Relates to the California Emergency Services Act. Provides for adding cyberterrorism within those conditions constituting a state of emergency and a local emergency.

Colorado

CO H 1200, Chap. 379
Concerns cybercrime, criminalizes using a computer to engage in prostitution of a minor, criminalizing skimming payment cards, and making changes to the penalty structure for cybercrime, changes the name of the crime computer crime to cybercrime, makes soliciting, arranging, or offering to arrange a situation in which a minor may engage in prostitution, by means of using a computer, computer network, computer system, or any part thereof, a cybercrime.

CO S 86, Chap. 319
Concerns the use of cyber coding cryptology for the transmission and storage of state records, requires the Chief Information Security Officer, the Director of OIT, the Department of State, and the Department of Regulatory Agencies to take certain actions to protect state records containing trusted sensitive and confidential information from criminal, unauthorized, or inadvertent manipulation or theft, makes an appropriation.

Florida

H.B. 755, Chap. 60
Relates to public records; provides an exemption from public records requirements for information obtained by persons or agencies from the First Responder Network Authority and information relating to the Nationwide Public Safety Broadband Network.

Source: www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

2018 Cybersecurity Legislation (continued)

FL H 1127, Chap. 65
Relates to public records; provides an exemption from public records requirements for certain records held by the Citizens Property Insurance Corporation which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents; provides retroactive application.

FL H 5001, Chap. 9
Makes appropriations, provides moneys for the annual period beginning July 1, 2018, and ending June 30, 2019, and supplemental appropriations for the period ending June 30, 2018, to pay salaries, and other expenses, capital outlay for buildings, and other improvements, and for other specified purposes of the various agencies of state government.

Iowa

IA H 2252, Chap. 1149
Changes the requirements for membership on the board of examiners for voting systems, allowing one member to have been trained in cybersecurity rather than requiring training in computer programming and operations.

Idaho

ID H 606, Chap. 142
Amends the Open Meeting Law, revises the definition of public agency, provides that the Cybersecurity Task Force or a committee awarding the state medal of achievement shall not constitute a public agency.

ID H 607, Chap. 258
Revises provisions relating to information technology services, provides for the Office of Information Technology Services, provides for the receipt of payment for services to units of state government, provides for advance payments and interaccount transactions, provides for the State Technology Authority, provides for responsibility of the integrated property records system.

Illinois

IL H 3342, Chap. 587
Makes changes in state programs that are necessary to implement the state budget; relates to cyber security.

IL H 5093, Public Act 1169
Creates the Information Security Improvement Act, creates the Office of the Statewide Chief Information Security Officer within the Department of Innovation and Technology, provides for the duties and powers of the Office, creates the position of Statewide Chief Information Security Officer to serve as the head of the Office.

IL H 5547, Chap. 914
Amends the State Auditing Act, provides that on a biennial basis, the Auditor General shall conduct a performance audit of state agencies and their cybersecurity programs and practices, with a particular focus on agencies holding large volumes of personal information, provides for the subjects to be assessed by the audit, provides for the issuance of an audit report.

IL HJR 59, Adopted
Creates the International Cybersecurity Task Force within the Commerce Commission to review the Joint Analysis Report from the U.S. Department of Homeland Security and the Federal Bureau of Investigation dated December 29, 2016 and entitled Grizzly Steppe - Russian Malicious Cyber Activity and develop strategies to either implement or reject the report recommendations, makes changes to who is to appoint to Co-Chair of the Task Force and to the membership of the committees.

IL S 2651, Chap. 623
Amends the Election Code; requires each election authority to submit information on the voting equipment used within their jurisdiction; provides for cybersecurity efforts; provides for mail in ballots.

Indiana

IN S 362, Chap. 126
Relates to the regulation of new water and wastewater systems, provides that a water or wastewater utility that begins providing service to the public, after a specified date, is subject to the jurisdiction of the State Utility Regulatory Commission, provides for rates and charges, and other matters, for a specified period, beginning on the day on which the water or wastewater utility begins providing service to the public.

Kansas

KS S 56, Chap. 97
Establishes the Cybersecurity Act, establishes the State Information Security Office, revises the membership of the Information Technology Executive Council.

Source: www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

2018 Cybersecurity Legislation (continued)

Kentucky

KY H 200, Chap. 169
Relates to the State/Executive Branch Budget: Detail Part I, Operating Budget, appropriates money to General Government.

KY H 244, Chap. 78
Establishes the Division of Enterprise Portfolios within the newly established Office of IT Architecture and Governance, establishes the Offices of Project Management, IT Services and Delivery, IT Architecture and Governance, the Chief Information Security Officer, KY Business One Stop, abolishes the Offices of Enterprise Technology, Infrastructure Services, Application Development, Chief Information Officer, and Information Technology Service Management.

Louisiana

LA H 601, Chap. 712
Revises provisions relating to election officials; prohibits the disclosure of specified information by the Registrar of Voters, Clerk of Court, and Department of State relating to the security and integrity of the state voter registration computer system, the election management system, and voting equipment.

Maryland

MD H 1331, Chap. 524
Requires the State Administrator of Elections to submit a report to the Department of Information 11 Technology within a specified period of time after becoming aware of a security violation involving an election system, requires certain information to appropriate persons and the State Administrator be forwarded within a certain period of time after receiving a report submitted by the State Board, authorizes the Secretary of Information Technology to require that certain information remain confidential.

MD H 1819, Chap. 566
Establishes the Cyber Warrior Diversity Program at Baltimore City Community College, Bowie State University, Coppin State University, Morgan State University, and the University of Maryland Eastern Shore, requires certain institutions of higher education to jointly hold a National Cyber Warrior Diversity Conference.

MD H 695, Chap. 304
Authorizes a public body to meet in a closed session to discuss cybersecurity, if the public body determines that public discussion would constitute certain risks.

MD H 874, Chap. 281
Requires the Executive Director of the Department of Legislative Services to ensure that the responsibilities of the Department are carried out, alters those offices that comprise the Department, alters certain duties of the Department to review certain reporting requirements, establishes the Office of Operations and Support Services to supervise certain support services to the General Assembly, provides that the Office of Policy Analysis is not required to prepare an analysis of certain enabling acts.

MD H 1331, Chap. 524
Requires the State Administrator of Elections to submit a report to the Department of Information 11 Technology within a specified period of time after becoming aware of a security violation involving an election system; requires certain information to appropriate persons and the State Administrator be forwarded within a certain period of time after receiving a report submitted by the State Board; authorizes the Secretary of Information Technology to require that certain information remain confidential.

MD S 204, Chap. 415
Establishes the Cybersecurity Public Service Scholarship Program, specifies the purpose of the Program, requires the Office of Student Financial Assistance in the Maryland Higher Education Commission to administer the Program, specifies certain eligibility requirements for an applicant to the Program, authorizes a certain scholarship award to be used at any eligible institution to pay for certain education expenses, requires a scholarship recipient to maintain a certain grade point average.

MD S 228, Chap. 578
Alters the definition of investment to include certain types of debt, authorizes buyers of certain technology to claim a credit against state income tax for purchase costs, authorizes qualified buyers to apply for the credit, requires a qualified buyer to attach a certain certificate to their income tax return, provides for the revocation and recapture of a credit under certain circumstances, makes a cybersecurity incentive tax credit subject to certain evaluations.

Source: www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

2018 Cybersecurity Legislation (continued)

MD S 281, Chap. 151
Alters the membership of the State Cybersecurity Council to include the State Administrator of Elections.

Michigan

MI H 4973, Chap. 68
Exempts public body records, documents, or information disclosable under freedom of information act.

MI H 5257, Chap. 95
Provides penalties for unauthorized possession or use of ransomware.

MI H 5258, Chap. 96
Provides sentencing guidelines for ransomware offenses.

MI H 6491, Chap. 690
Enacts the Insurance Data Security Model law; establishes the exclusive standards, for this state, applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the director.

MI S 149, Chap. 586
Relates for the school aid appropriations budget, provides the sum of the final audited count from the supplemental count day of pupils in grades K to 12 actually enrolled and in regular daily attendance in the community district for the immediately preceding school year plus the final audited count from the supplemental count day of pupils in grades K to 12 actually enrolled and in regular daily attendance in the education achievement system for the immediately preceding school year.

MI S 941, Chap. 227
Enacts appropriations in School Aid Fund for the Marshall Plan for Talent.

Missouri

MO H 1355
Establishes a joint committee of the general assembly, which shall be known as the "Joint Committee on Disaster Preparedness and Awareness"; requires the committee to make a continuous study and investigation into issues relating to disaster preparedness and awareness including, natural and man-made disasters, state and local preparedness for floods, state and local preparedness for tornadoes, blizzards, and other severe storms, food and energy resiliency and cyber-security.

Nebraska

NE L 757
Revises provisions of the Credit Report Protection Act and the Financial Data Protection and Consumer Notification of Data Security Breach Act, requires substantially similar types of a security product that provides the same level of protection to a consumer's credit report as that provided under the Credit Report Protection Act, prohibits an agency using a similar type of security product from charging a fee to a consumer, requires maintenance of reasonable security procedures and practices.

New Hampshire

NH H 1335, Chap. 63
Prohibits state agencies from using software developed by Kaspersky Labs.

Ohio

OH S 273, Chap. 134
Clarifies the definition of an insurance rating agency; requires each licensee to develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment; relates to a domestic surplus lines insurer.

Puerto Rico

PR H 246

South Carolina

SC H 4655, Act 171
Enacts the State Insurance Data Security Act; requires a licensee to develop, implement and maintain a comprehensive information security program based on the licensee's risk assessment and to establish certain requirements for the security program; provides minimum requirements for a licensee's Board of Directors, if applicable; requires a licensee to monitor the security program and make adjustments if necessary; provides that the licensee must establish an incident response plan; relates to reports.

SC H 4950
Makes appropriations. Requires all state agencies to adopt and implement cyber security policies, guidelines and standards developed by the Department of Administration. The department may conduct audits on state agencies except public institutions of higher learning, technical colleges, political subdivisions, and quasi-governmental bodies as necessary to monitor compliance with established cyber security policies, guidelines and standards.

Source: www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

2018 Cybersecurity Legislation (continued)

Utah

UT H 174, Chap. 125
Changes the composition of the Utah Digital Health Service Commission; increases the number of members on the commission; creates an additional category for representation; increase the number of members required for a quorum; adds information security to the duties and responsibilities.

UT S 242, Chap. 444
Amends provisions relating to cybercrime.

Virginia

VA H 727, Chap. 52
Relates to Freedom of Information Act, relates to exclusion of records relating to public safety, clarifies the exclusion from mandatory disclosure of information relating to a safety program plan pursuant to Federal Transit Administration regulations, makes a nonsubstantive correction.

VA H 1221, Chap. 775
Relates to Virginia Information Technologies Agency, relates to additional duties of the Chief Information Officer, relates to cybersecurity review, requires the CIO of the Information Technologies Agency to conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures.

VA H 5002 a, Chap. 2
Relates to Budget Bill, appropriations of the Budget submitted by the Governor of Virginia in accordance with the provisions of Section 2.2-1509, Code of Virginia, and to provide a portion of revenues for the two years ending respectively on the thirtieth day of June, 2019, and the thirtieth day of June, 2020.

VA S 657, Chap. 741
Relates to the Freedom of Information Act, relates to exclusion of records relating to public safety, excludes from mandatory disclosure under the Freedom of Information Act information held by the State Commercial Space Flight Authority, provides for information that is categorized as classified, or sensitive but unclassified, including national security, defense, and foreign policy information.

VA S 966, Chap. 296
Relates to electric utility regulation, provides for grid modernization and energy efficiency programs, provides for rate review proceedings and transitional rate periods, provides for energy storage facilities, relates to electric distribution grid transformation projects, and wind and solar generation facilities, relates to coal combustion by product management, relates to undergrounding electrical transmission lines, relates to fuel factor.

Vermont

VT H.B. 764, Chap. 171
Relates to data brokers and consumer protection.

VT H 16a, Chap. 11
Makes appropriations for the support of government, cybersecurity, financial education, and vital records; provides for the Workforce Education and Training Fund; provides for the One Time Clean Energy Development Fund; provides for Medicaid programs; provides for education funding; provides funding for social services programs; provides for certain taxation

Washington

WA H 2406, Chap. 218
Concerns election security practices around auditing and equipment, adds options to the auditing process for local elections administrators, concerns maximizing the security benefits of having locally run, decentralized counting systems.

WA S 6032, Chap. 299
Makes supplemental operating appropriations, relates to the general fund.

West Virginia

WV S 495, Chap. 128
Relates to commercial insurance rates, designates cybersecurity insurance coverage as exempt from the requirements of filing rates with the insurance commissioner.

Wyoming

WY H 1, Chap. 134
Makes appropriations for the fiscal biennium commencing July 1, 2018 and ending June 30, 2020, provides definitions, provides for appropriations and transfers of funds for the period of the budget and for the remainder of the current biennium as specified, provides for carryover of certain funds beyond the biennium as specified, provides for employee positions as specified.

Source: www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

The California Consumer Privacy Act of 2018

Perhaps the most significant regulatory development in the area of data protection was the passage in late June 2018 of the California Consumer Privacy Act (CCPA). The CCPA was hastily passed as a compromise to avoid a more extensive ballot initiative. Weeks later, in an effort to correct and clarify several drafting errors, the California legislature passed Senate Bill 1121 which was subsequently signed into law by Governor Brown.

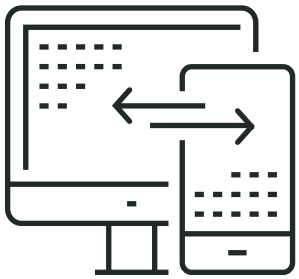
The CCPA borrows substantially from the EU GDPR and establishes stringent obligations on businesses with regard to the collection, retention, use, disclosure and disposal of consumers' personal information and provides for private rights of action and enforcement by the California Attorney General. Despite the passage of the CCPA (and amendments), the controversy and uncertainty surrounding it continues into 2019. Industry groups have pushed for more substantial changes in the law, beyond the already approved technical revisions. These proposed changes include delaying implementation, narrowing the definition of "personal information," and clarifying the definition of "consumer." A group of privacy advocates has responded by urging the legislature to reject the industry group proposals and encouraging it to adopt additional protections for consumers.

Although the CCPA does not become effective until January 1, 2020, and it is likely that the provisions set forth in the final law will be different from those reflected in the current version, businesses would be well-advised to begin addressing its requirements. Businesses will need to start data mapping and recordkeeping by January 1, 2019 to be in compliance on the effective date. A bill modeled on the CCPA was introduced in New Jersey, but It is too early to determine if other states will follow California's lead and establish similar consumer privacy regulations.

State Laws & Legislature (Continued)

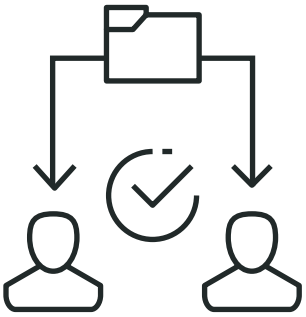
California - Internet of Things Law

California also passed an "Internet of Things" (IoT) law" in 2018, the first of its kind in the nation. The law requires a manufacturer of a "connected device" to "equip the device with a reasonable security feature or features designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." The law does not create a private right of action for violations but does grant enforcement authority to state and local officials.



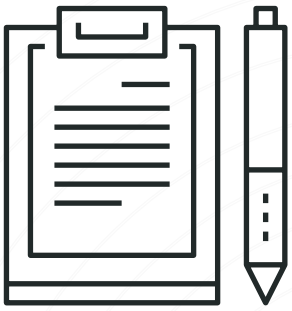
Vermont - Data Broker Law

In 2018 Vermont became the first state to enact a data broker law. Businesses falling within the definition of "data broker"—a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship—are required to register annually with the Secretary of State, incorporate standard security measures in handling personally identifiable information, and notify authorities of security breaches.



Ohio - Senate Bill 220

Also in 2018, Ohio enacted Senate Bill 220 (Ohio Data Protection Act). The purpose of the law is to provide businesses with a legal incentive to adopt and maintain written cybersecurity programs and is the first such state law of its kind.



Push For Federal Data Protection Law

While state activity in the area of consumer data privacy and security remains high, several factors have contributed to a more vigorous push for a national standard on consumer data protection. This heightened attention on a common data privacy and security framework has been attributed to factors such as the passing of the May 25, 2018 effective date of the GDPR, the passage of the CCPA in California, and recurring news of significant and high-profile data breaches, such as the Marriott "data security incident" disclosed in November 2018.

In September, the Senate Committee on Commerce, Science, and Transportation convened a hearing to "examine privacy policies of top technology and communications firms, review the current state of consumer data privacy, and offer members the opportunity to discuss possible approaches to safeguarding privacy more effectively." Representatives from AT&T, Google, Amazon, Twitter, Apple and Charter Communications offered testimony and support for a federal data protection law which would preempt state laws. In October, the Committee held an additional hearing which included input from parties outside of the technology industry, including consumer advocates and consumer protection authorities.

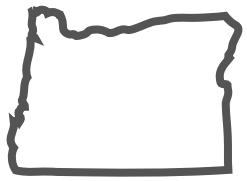
Concurrently with the Committee hearing, the National Telecommunications and Information Administration (NTIA), within the US Department of Commerce, issued its Request for Comments on Developing the Administration's Approach to Consumer Privacy. In its Request for Comments, the NTIA set out a list of proposed privacy "outcomes" which are intended to serve as the foundation of a risk-management approach to consumer privacy protection. These outcomes include Transparency, Control, Reasonable Minimization, Security, Access and Correction, Risk Management, and Accountability. The Request for Comments also outlines a list of "High-Level Goals for Federal Action" which includes a recommendation that the FTC be designated as the primary federal agency for consumer privacy enforcement. The NTIA subsequently released the comments it received from a multitude of individuals, businesses, coalitions, governmental agencies, foundations, associations, and advocacy organizations.

Push For Federal Data Protection Law (continued)

A number of industry groups have spoken in favor of a federal standard for consumer privacy and data protection. The Internet Association, a trade association representing global internet companies, issued a response to the NTIA's Request for Comments, stating, in part, that it supports "a modern approach to privacy regulation that meets consumer demands and provides a clear and consistent framework from coast to coast". The Interactive Advertising Bureau sent a letter to the Senate Committee on Commerce, Science, and Transportation, expressing its position that a "uniform Federal privacy standard could provide clarity, market certainty, and add fuel to future innovation". BSA/The Software Alliance, an advocate for the global software industry, has issued its own proposed Privacy Framework in support of national data privacy standards. Google recently published its "Framework for Responsible Data Protection Regulation" in support of "comprehensive, baseline privacy regulation". Other technology companies and groups expressing support for a comprehensive national privacy framework include Facebook, Google, Microsoft, Apple, Intel, the Information Technology Industry Council, and Business Roundtable.

Consumer and privacy advocacy groups were predictably concerned that the proposals offered by technology and industry would not provide adequate protections to individuals and presented their own recommendations for a set of privacy principles. In November, a coalition of 34 advocacy groups released a set of principles they believe should be reflected in any future federal U.S. privacy legislation. The Electronic Frontier Foundation (EFF), which describes itself as the "the leading nonprofit organization defending civil liberties in the digital world", was not part of the coalition, but submitted its own set of proposed privacy principles.

Will federal privacy legislation be passed in 2019? A number of forces are driving the push for a national data privacy framework, including the GDPR, the California Consumer Privacy Act, and a seemingly endless series of reports of major data breaches arising in jurisdictions from around the globe. Senator Ron Wyden (Oregon) has proposed such legislation in the draft Consumer Data Protection Act. The bill would expand the Federal Trade Commission's enforcement authority in the area of privacy protection, provide for the creation of a national Do-Not-Track system for consumers, and establish substantial penalties, including jail time for executives.



What Do Businesses Need To Do?

Keeping up with the constantly changing regulatory landscape is not easy, and proves the need for a systematic and pragmatic compliance system. Such a system should allow the business to ensure compliance, while avoiding excessive constraints on the organization.

Edgile is a leader in providing businesses with tools to stay on top of this rapidly changing regulatory environment. Edgile's iGRC Managed Content Service tracks over 70 state, federal, global and industry-specific compliance and regulatory requirements, including PCI, SOX, NIST, NYDFS, FFIEC and HIPAA.

The iGRC "risk register" reduces the regulatory burdens on businesses by:

- **Automatically identifying and updating all applicable legal, statutory and regulatory requirements at all levels including international, federal, and state on a quarterly basis.** Keeping track of new regulatory rules and guidance from state, federal, and industry-specific authorities is an intensive effort requiring both legal expertise and thorough knowledge of an organization's internal controls.

- **Providing a proven methodology to translate regulatory requirements into simple control plans that system administrators, application owners, and business risk owners can understand and follow.** We commonly see organizations that have identified their needed cyber and privacy controls, but struggle with operationalizing those controls. Their compliance systems failed to go "the last mile" leaving the organization exposed to regulatory and cyber risk. Edgile's methodology systematically maps regulatory requirements to system-specific controls, while keeping it simple and pragmatic for the business.

- **Using a "strategy-first" approach to regulatory compliance management.** Today's risk managers need to envision comprehensive solutions instead of addressing checkboxes. We advocate risk officers always start with a comprehensive cyber and privacy strategy that properly aligns risk objectives with business objectives. Such strategies are key to building the cross-functional alignment and risk ownership that lead to a successful cyber security program.

Supporting Resources

1) *iGRCContent Service for Manual or Automatic Regulatory Compliance*

2) *Technology Diagnostics For Financial Services*

3) *How The C-Suite is Blinded by Compartmentalized Compliance Efforts*

4) *The Top 6 Compliance and Security Mistakes US Banks Make When Moving To The Cloud*

Contact Edgile

West

Brian Rizman
Managing Director
brian.rizman@edgile.com
(908) 489-3293

Central

David Deckter
Partner
david.deckter@edgile.com
(312) 371-6363

East

Geoff Hauge
Partner
geoff.hauge@edgile.com
(646) 469-9008

About Edgile

Edgile is the trusted cyber risk and compliance partner to the world's leading organizations, providing consulting, managed services, and harmonized regulatory content. Our strategy-first model optimizes IAM, GRC, and cybersecurity both on-premises and in the cloud. By transforming risk into opportunity, we secure the modern enterprise through solutions that increase business agility and create a competitive advantage for our clients.

For more information about Edgile,
visit www.edgile.com.