

Critical Infrastructure:

2018 Cybersecurity Year in Review/2019 Year Ahead Analysis

January 24, 2019

Van Ness Feldman LLP

Van Ness Feldman LLP

"Cyber resilience is not solely a concern for companies, it's a societal and government stake."[1]

- Stephane Nappo, Global Chief Information Security Officer at Société Générale International Banking

EXECUTIVE SUMMARY

We are pleased to provide our 2nd Annual Cybersecurity Year in Review/Year Ahead Analysis to clients and friends of the firm. Van Ness Feldman's cybersecurity team has consolidated and summarized important cyber related developments from 2018, as well as provided some analysis about the direction cybersecurity issues may take in 2019 as they relate to the interests of firm clients. Our team continues to track both cybersecurity law and policy developments in a wide range of critical infrastructure areas, chief among them are energy, water, and health, as well as highlighting a handful growing fields.

Specifically, this document summarizes new regulatory initiatives undertaken by federal agencies and Congress. For example, activities at the Federal Energy Regulatory Commission ("FERC") and North America Electric Reliability Corporation ("NERC") and their impact on electric utility clients. The review also discusses updates provided by the Transportation Security Administration ("TSA") for natural gas pipelines, and the continued debate about the efficacy of the agency's regulatory posture. With respect to the water sector, the review covers the implications of America's Water Infrastructure Act of 2018, which requires all community water systems serving more than 3,300 to conduct a risk and resilience assessment that must consider cybersecurity threats. Lastly, in the health sector, we review new cybersecurity initiatives by the Department of Health and Human Services and the agency's response to bipartisan criticism of an earlier cyber threat report.

This document also addresses cybersecurity related advancements in emerging areas such as privacy, data security and autonomous vehicles. While Congress grapples with crafting an overarching privacy law, several states have lead the way enacting legislation to protect their citizens. On the international front, companies remain watchful of the impact of the European Union General Data Protection Regulation ("GDPR").

Finally, in keeping with the firm's foundational policy and government advocacy services, our team has tracked the key legislative developments that impact cybersecurity. Despite the anecdotes of gridlock, Congress enacted several laws impacting funding for and the efficacy of cybersecurity programs. Members offered even more bills to advance pipeline cybersecurity and other initiatives, however with the close of the 115th Congress, many of these bills will need to be reintroduced in 2019.

[1] 2018 Global CISO of the year.

2018 was an action-packed year in terms of new and different approaches to addressing some of the country's most imminent cybersecurity threats and we expect even more innovation and discussion in 2019. VNF's cybersecurity team will continue to keep you well informed in this New Year. In the interim, if you have any questions or need more information about the topics below, please do not hesitate to contact us.

ENERGY SECTOR

Electric Subsector

2018 Developments

The year 2018 saw continued dedication on the part of the Federal Energy Regulatory Commission ("FERC" or the "Commission") and North America Electric Reliability Corporation ("NERC") to finalize a suite of cybersecurity proposed rules announced in late 2017 and early 2018. Specifically, FERC and NERC approved rules relating to security management controls, cybersecurity incident reporting, and supply chain risk. For analysis of the latter two rulemakings please see the following VNF client alerts: *FERC Raises the Threshold for Cyber Incident* Reporting and *Significant Supply Chain Management Changes on the Horizon for Electric Utilities*.

The proposed security management control Critical Infrastructure Protection ("CIP") reliability standard CIP-003-7, which was covered in our last year-end report, was not approved by FERC in its entirety. The notice of proposed rulemaking sought to modify the CIP standard so that it provided clear criteria for electronic access controls for low impact Bulk Electric System ("BES") cyber systems and also addressed the need to mitigate the risk of malicious code that could result from third-third party transient devices (such as thumb drives, laptops, and other portable devices that can be connected and disconnected from the network). While FERC's final rule did ultimately adopt mandatory security controls for transient devices used at low impact BES's, the Commission declined to adopt the proposed directive relating to electronic access controls. In light of the comments received, the Commission ultimately decided that the access controls that had been proposed did not provide the clarity necessary to establish compliance expectations. Instead, FERC *clarified* electronic access control obligations and directed NERC to conduct a study to determine whether the electronic access controls adopted by entities in response to the clarifications in CIP-003-7 provide adequate security.

Beyond these regulatory developments, FERC demonstrated its commitment to improving electric sector cybersecurity discussing the issue in depth at a Technical Conference held on July 31, 2018. At the Conference, the Commissioners acknowledged the critical role that cybersecurity plays in ensuring the reliability of the electric grid and asked industry representatives to identify where the CIP standards have been successful and areas in which the CIP reliability standards must be improved. The Commissioners' interest in these matters suggests that FERC is committed to reviewing the current

standards to ensure that they strike a balance between providing a "benchmark" standard for industry to meet while not stifling industry innovation in the cyber field.

2019 Look Ahead

NERC and FERC proposed and approved cyber-related rules in 2018 at a rapid pace -the three final rules mentioned above yielded four new CIP standards approved in 2018 alone- and we expect both agencies to build on this regulatory momentum in 2019 to continue supporting the electric industry as it works toward closing the existing regulatory gaps, expanding programs that currently work, and wrestling with corporate issues. ; In addition to the approval of these 2018 CIP standards, FERC called on NERC to revise and or create standards relating to cyber incident reporting. With regards to existing regulatory gaps, we anticipate that FERC and NERC will work to continue refining the CIP standards to better meet industry needs while also fostering cybersecurity in the bulk electric system. Specifically, FERC and NERC will have to determine how to best mitigate the ongoing struggle to develop standards at the pace necessary to keep up with the rapidly changing cyber field. Achieving this objective will entail further work on the existing cybersecurity standards to build-in the appropriate amount of flexibility so that utilities can comply with the standards while also dealing with high volumes of cyber attacks.

As FERC and NERC work together to revise the CIP standards, they may consider moving toward a more outcome-based approach, rather than a prescriptive approach by setting expectations and leaving implementation measures to the discretion of utilities themselves. As these agencies work to close regulatory gaps, they will also work to bolster programs and initiatives that are already successful. One example of such a program is NERC's Cybersecurity Risk Information Sharing Program ("CRISP"), which has been embraced by industry and shown to be an effective tool in promoting information sharing. We expect NERC to both expand the program and broaden its scope.

Lastly, as utilities face monetary restrictions and limited resources due to corporate investment conflicts, the Commission has indicated that it will support utilities in recovering cyber related cost through their rates. While it is unclear what the scope and form this recovery may take, as the number of threats and regulations increase, we predict that the matter will be raised in a proceeding before the Commission this year.

Natural Gas Subsector

2018 Developments

In 2018, the natural gas pipeline industry found itself under increased scrutiny as its regulatory cyber scheme was examined. This scrutiny has provided the natural gas sector with an opportunity to demonstrate that pipeline companies already have the necessary protocols and procedures in place in the

event of a cyber-attack and that the current level of regulatory oversight is adequate. The Transportation Security Administration ("TSA")—the federal agency currently responsible for overseeing cybersecurity for natural gas pipelines in the United States—updated its cybersecurity guidelines for interstate natural gas pipelines to better align with guidance issued by the National Institute of Standards and Technology (NIST). (For more in depth analysis see *Updated TSA Guidelines Suggest New Approach for Pipeline Cybersecurity | Van Ness Feldman LLP*). Nonetheless, critics expressed concern that the voluntary nature of that guidance—as well as the fact that the guidance ignored important supply-chain risk management measures—leaves the natural gas sector ill prepared to respond to a cyber-attack levied by a sophisticated actor.

These critics—which include multiple White House and agency officials, as well as leaders in the electric sector—spent 2018 advocating for the promulgation of more stringent standards to protect the interconnectivity of the electric grid. The FERC acknowledged these concerns and expressed their own concerns. In fact, FERC Chairman Neil Chatterjee and Commissioner Richard Glick, went so far as to publish an op-ed in which they stated that TSA, due to a lack of resources, is not equipped to take on the level of regulatory responsibility required and suggested that the Department of Energy assume responsibility for pipeline cybersecurity. Likewise, in a December 2018 Report issued by the Government Accounting Office ("GAO") titled "Actions Needed to Address Significant Weakness in TSA's Pipeline Security Program Management," the GAO identified several issues with the TSA's current approach to regulating cybersecurity. Specifically, the GAO found that the 2018 update to the Pipeline Security Guidelines lacked the clarity necessary for pipelines to determine the criticality of their facilities. The GAO report also identified critical deficiencies in the TSA's current process, including staffing limitations, the absence of a documented process for revising and reviewing the Pipeline Security Guidelines, the lack of measurable targets for pipelines to work towards, and the TSA's failure to follow up on the recommendations that it issues. The GAO ultimately made 10 recommendations to the TSA to improve its pipeline security program management.

In its response to the GAO report, the Interstate Natural Gas Association of America ("INGAA") indicated that cybersecurity remains a priority of the organization and its members. The organization cited several new proactive initiatives undertaken in partnership with federal agencies that were not addressed in the report, including cybersecurity assessments of pipelines to evaluate practices and attempt to stay ahead of the ever-changing cyber threats. Most importantly, however, industry leaders and INGAA cautioned not to apply a "one-size fits all" approach to cybersecurity across the energy sector and emphasized the need for flexibility rather than mandatory standards that are "often outdated as soon as they are introduced."

2019 Look Ahead

It has become increasingly clear that there will be continued debate about TSA's current regulatory scheme as the jurisdictional battles between FERC and TSA over various cyber-related pipeline issues progress in the months ahead. The natural gas industry is eager to avoid the implementation of stricter guidelines or mandatory standards, asserting that the adherence to prescriptive rules is an inefficient methodology for responding to evolving threats. However, developments like the GAO's report, increasing pressures from FERC and other stakeholders and changes in the legislative landscape will make that harder in 2019.

In Congress, Representative Frank Pallone (D-NJ), co-author of the letter requesting the GAO report and an avid supporter of increased pipeline supervision, assumed the Chairmanship of the House Energy and Commerce Committee with Democrats regaining the majority in the chamber. The Committee is likely to hold hearings on pipeline cybersecurity and could put forward new legislation to standardize best practices. Already, legislation has been introduced in this Congress (the Pipeline and LNG Facility Cybersecurity Preparedness Act) that would convey upon DOE the authority to establish a program promoting cyber and physical security for pipelines. The bill is identical to a version that cleared the Energy and Commerce Committee by voice vote last year under Republican leadership, and it is likely to at least pass the House in 2019. Given that the natural gas industry has expressed a desire for the authority to remain with TSA at its current level of involvement, the agency may respond by attempting to implement the GAO's recommendations and seek to have its Guidelines incorporate the missing important elements of the NIST Framework relating to supply chain resiliency in 2019.

Water Sector

2018 Developments

2018 has been a year of risk recognition for the Water Sector. Harkening back to 2014, the NIST Cybersecurity Framework , issued in response to the 2013 Executive Order 13636 - Improving Critical Infrastructure Cybersecurity, took on greater meaning in the context of actual attacks in the water sector.

In 2018, the American Water Works Association's ("AWWA") *Cybersecurity Risk and Responsibility In the Water Sector Report* ("Risk and Responsibility Report") provided examples of actual water sector attacks that took place in 2018:

- The utilities of the City of Atlanta were disrupted by a ransomware attack in March 2018.
- In another ransomware attack on a water utility affected through spear-phishing locked the utility out of its own systems, demanding the equivalent of $25,000 in Bitcoin to recover access.

- Cybercriminals exploited vulnerability in a remote wireless Internet connection for operations for approximately two months, and also exploited a hard-coded factory password.
- Cybercriminals exploited antiquated computer systems to gain access to valve and flow operations and were able to manipulate the water flow and amount of chemicals used to treat the water.
- Iranian activists exploited a vulnerability to identify an unprotected computer that controlled sluice gates and other functions of the Bowman Dam.

On October 23, 2018, America's Water Infrastructure Act ("AWIA") was signed into law. The law requires community water systems serving more than 3,300 people to develop or update risk and resilience assessments ("RRAs") and emergency response plans ("ERPs"). The law includes components that the risk assessments and ERPs must address, and establishes deadlines by which water systems must certify to the US Environmental Protection Agency ("USEPA") completion of the risk assessment and ERP. The assessments required under SEC. 1433(a)(1)(A) of the AWIA include building resilience from malevolent acts and natural hazards of

- pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;
- the monitoring practices of the system;
- the financial infrastructure of the system;
- the use, storage, or handling of various chemicals by the system; and
- the operation and maintenance of the system.

"*Resilience*" is defined by the AWIA as: *the ability of a community water system or an asset of a community water system to adapt to or withstand the effects of a malevolent act or natural hazard without interruption to the asset's or system's function, or if the function is interrupted, to rapidly return to a normal operating condition.*

To assist water utilities with these new mandates and build resilience, AWWA's Risk and Responsibility Report also included steps for water utilities to undertake in an effort to not only protect their systems and operations, but customer data as well.

2019 Look Ahead

With the risk and reliance assessments required by the AWIA, as well as the increased publicity and understanding of potential vulnerabilities, water utilities will continue to assess and attempt to address

cyber risks, at a time that utilities are modernizing operational systems to connect to not only each other, but also corporate networks, the internet, and the cloud. Areas of focus for assessments will likely include external access points to utility network, use of remote access, management of switches, routers, business systems (workstations and servers), employee training, redundant security checks, and handling of private information.

The AWIA requires the new RRA for all providers serving more than 3,300 customers. Under Sec. 1433(a)(2) of the AWIA, by no later than August 1, 2019, EPA will consult with federal, state and local agencies and then provide baseline information on malevolent acts of relevance to utilities. In 2019, utilities will be engaged in reviewing the EPA criteria and beginning assessments in order to be able to certify to EPA that its system has conducted the RRA between March 31, 2020 and June 30, 2021 (based on size). See Sec. 1433(a)(4) of the AWIA

Under Sec 1433(b) of the AWIA that within 6 months after completion of the RRA, each provider must prepare of revise its ERP to include:

- strategies and resources to improve the resilience of the system,
- plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard
- actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and
- strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

In 2019, in anticipation of the certification requirements starting in 2020, public water utilities subject to state public records acts, may also be considering how to limit vulnerability of disclosure of sensitive portions of their RRAs and ERPs that might be triggered by public disclosure requests of those documents.

Health Sector

2018 Developments

Healthcare-related cybersecurity issues occupied a significant portion of the House Energy & Commerce Committee's agenda in 2018. On June 5, 2018, Committee Chairman Greg Walden (R-OR) and Ranking Member Frank Pallone (D-NJ)—together with Senate Health, Education, Labor & Pensions Chairman

Lamar Alexander (R-TN) and Ranking Member Patty Murray (D-WA)—authored a letter to the Department of Health and Human Services ("HHS") to raise concerns about the department's 2017 Cyber Threat Preparedness Report ("CTPR") which outlined HHS's roles and responsibilities to address cyber threats in the healthcare sector. Specifically, the Members were interested in understanding the operational status of the Healthcare Cybersecurity and Communications Integration Center ("HCCIC"), identifying the individual leading the HCCIC, and learning more about the HCCIC's capabilities and responsibilities. The letter also questioned how HHS manages in the dual roles of regulating the health care sector and serving as the Sector Specific Agency ("SSA") responsible for leading and providing guidance under the national critical infrastructure protection model. On October 4, 2018, HHS responded to the House and Senate letter stating that it would update the CTPR by February 2019 to provide the information requested by Congress.

In October 2018, HHS officially launched the Health Sector Cybersecurity Coordination Center ("HC3"), which will work with stakeholders, including practitioners, organizations, and cybersecurity information sharing organizations to understand the cyber threats facing the health sector and to provide information and approaches on how the sector can better defend itself. HC3 will report to the Department of Homeland Security ("DHS") on cybersecurity threats, profiles, and preventive strategies. Late in 2018, HHS published in the *Federal Register* a Request for Information ("RFI") on how the Health Insurance Portability and Accountability Act ("HIPAA") Rules—especially the HIPAA Privacy Rule—could be modified to further the department's goal of promoting coordinated, value-based healthcare. HHS is interested in hearing from stakeholders about (i) encouraging information-sharing for treatment and care coordination; (ii) facilitating parental involvement in care; (iii) addressing the opioid crisis and serious mental illness; (iv) providing an accounting for disclosures of Protected Health Information (PHI) for treatment, payment, and health care operations; and (v) changing the current requirement for certain providers to make a good-faith effort to obtain an acknowledgment of receipt of the Notice of Privacy Practices. Comments on the RFI are due by February 11, 2019. In addition to examining HHS, the Energy & Commerce Committee issued a Request for Information to the private sector to learn more about the use of legacy technologies in healthcare and how these technologies have contributed to healthcare cybersecurity challenges.

2019 Look Ahead

The 2019 Congress brings new leadership to the House and Senate Committees with jurisdiction over healthcare cybersecurity and data privacy issues. With Democrats taking control of the House of Representatives, Rep. Frank Pallone (D-NJ) will assume the Chairmanship of the House Energy & Commerce Committee and has expressed support for examining meaningful privacy and data security protections for consumers. Rep. Diana DeGette (D-CO) is expected to serve as Chair of the Energy & Commerce Subcommittee on Oversight & Investigations which will examine these policies.

Sen. Roger Wicker (R-MS), the new Chairman of the Senate Commerce, Science & Transportation Committee, is interested in cybersecurity and data privacy policy and has previously discussed the need for Congress to pass a comprehensive consumer data protection law that would preempt state laws to ensure that consumers maintain the same protections across state lines. Other Senators on the Committee, including Sen. John Thune (R-SD), the former Chair of the Committee; Sen. Jerry Moran (R-KS); and Sen. Blumenthal (D-CT), are working on data privacy legislation which could provide the Federal Trade Commission ("FTC") with additional authority in this area.

In the Administration, HHS is expected to take the comments to the HIPAA RFI and begin the rulemaking process for updating HIPAA regulations. The FTC is also expected to increase their oversight of privacy and security practices for consumer data.

Privacy & Data Security

2018 Developments

Issues of privacy and data security took center stage in 2018. Multiple companies experienced major (and very public) data breaches, resulting in both unauthorized access to millions of users' personally identifiable information, as well as significant economic and legal liability for the affected companies. In addition, several jurisdictions took steps to implement comprehensive privacy laws aimed at vesting individuals with some degree of control over the collection and processing of their personal data. The most significant development on this front occurred on May 25, 2018, when the European Union General Data Protection Regulation ("GDPR") went into effect. Among other requirements, the GDPR (i) mandates that a company must provide a legal justification for the collection and processing of data of EU citizens, even if those citizens are located in jurisdictions outside of the EU (such as the United States); (ii) requires that a company notify authorities of a data breach within 72 hours; and (iii) provides EU citizens the right to request that a company delete certain personal information that has been collected. If a company is found to violate any one of these rules, then European regulators now have the authority to impose fines of up to 4 percent of a company's annual global revenue.

Returning stateside, on June 28, 2018, the State of California made headlines when it enacted the California Consumer Privacy Act ("CCPA"), a comprehensive GDPR-like privacy law that will bring fundamental privacy protections to 40 million Californians starting in 2020. Once the law goes into effect, Californians will have the right to know which of their information companies are collecting and to opt out of having companies share that data with third parties. The CCPA will also provide California consumers with a private right of action to sue any companies that violate the law. Like the GDPR, the CCPA will apply to any company that is processing data of California consumers, regardless of location.

Beyond these comprehensive measures, the year 2018 also saw several other U.S. jurisdictions take notable steps that will have privacy implications in years to come. For example, Ohio chose to pursue a less consumer-centric policy and enacted a first-in-the-nation "safe harbor" law that provides a liability shield against consumer data breach claims where a company has implemented a written cybersecurity program that "reasonably conforms" to one of 11 industry standard cybersecurity frameworks, including several frameworks promulgated by the National Institute for Standards and Technology ("NIST"). Also in 2018, Alabama enacted a state data breach notification law, becoming the last state in the nation to take such a measure. Under the Alabama law, where a company determines that a security breach is "reasonably" likely to cause substantial harm to affected individuals, that company must provide written notice to affected individuals within 45 calendar days. Notice to all consumer reporting agencies and to the Alabama Office of the Attorney General is also required "without unreasonable delay" if it is determined that over 1,000 Alabama residents were impacted.

The year 2018 also saw growing interest from Congress over privacy and data security issues, particularly following the announcement of massive data breaches at both Facebook and Marriott. In the wake of these events, bipartisan calls for comprehensive national privacy legislation escalated. Among the most vocal advocates for a national privacy law were Senators Ron Wyden (D-OR) and Brian Schatz (D-HI), both of whom introduced proposed legislation late in 2018. As calls from within Congress for national privacy legislation have grown louder, so too have external endorsement for a national privacy law, particularly as industry has begun to recognize the potential challenges—and costs—associated with complying across multiple jurisdictions. To that end, 2018 saw both the Internet Association and the U.S. Chamber of Commerce release principles for a national privacy law.

Not to be outdone, the executive branch also undertook efforts to start crafting a coherent narrative with respect to personal privacy. Specifically, on September 26, 2018, the National Telecommunications and Information Administration (NTIA) published in the *Federal Register* a request for public comments on developing the Trump Administration's "Approach to Consumer Privacy." Likewise, on November 14, 2018, NIST published in the *Federal Register* a notice and request for information (RFI) seeking public comments on NIST's efforts to develop a Privacy Framework. NIST's objective is to "collaboratively develop the Privacy Framework as a voluntary, enterprise-level tool that could provide a catalog of privacy outcomes and approaches to help organizations prioritize strategies that create flexible and effective privacy protection solutions, and enable individuals to enjoy the benefits of innovative technologies with greater confidence and trust."

Within the judicial branch, the U.S. Supreme Court in June 2018 issued its groundbreaking opinion in *Carpenter v. U.S.*, in which the Court held that the government generally must obtain a warrant to access a record of a person's historic cell phone location information (known as cell-service location information or "CSLI"). Finding that cell phones constitute an indispensable element of modern life,

Chief Justice Roberts—the author of the majority opinion—wrote that CSLI can be used for tracking purposes "by dint of its operation, without any affirmative act on the part of the user beyond powering up"—a functionality that distinguishes cell phone tracking from more traditional investigative techniques. Although the Court characterized *Carpenter* as a "narrow" decision—declining to "disturb the application of [existing precedent] or call into question conventional surveillance techniques and tools such as security cameras"—the case provides valuable context into how the Court thinks about the privacy implications of emerging technologies and the decision may prove instructive to an agency contemplating thoughtful regulation to address personal privacy concerns that arise incident to the incorporation of new technologies into specific industries.

More generally, 2018 witnessed more action by federal and state legislators and regulators to prescribe industry- and device-specific rules governing devices operating within the Internet of Things ("IoT"). Supported by efforts by the Federal Communications Commission to push for expedited and scaled deployment of fifth generation wireless technology ("5G"), as well as rapid developments in artificial intelligence, a host of new technologies—from autonomous cars and drones to smart ovens—joined the network. Recognizing the ability of these devices to store vast quantities of personal data—and the potential privacy incursions wrought by these devices—agencies, including NIST, the Food and Drug Administration ("FDA") and the National Highway Transportation Safety Administration ("NHTSA"), began to issue guidance on IoT privacy and security.

2019 Look Ahead

Many of the dominant themes to emerge in 2018 are likely to persist into 2019 and beyond. On the international front, in 2019, Europe will remain the center of the privacy universe as we are likely to see continued focus on GDPR and its application to US based companies. In particular, there is likely to be an uptick in investigatory and enforcement activities by European regulators, given that companies have now had over six months to comply with the regulation. Thus, 2019 may witness the first assessment of significant penalties under the law, which would signal to the world that Europe is committed to holding companies accountable. Also in 2019, the European Data Protection Board, the multinational EU body charged with ensuring consistent application of the GDPR, will likely promulgate interpretive guidance related to key GDPR provisions. Companies will need to watch closely for release of this guidance and ensure that they amend their GDPR strategies as necessary to ensure compliance with that guidance. In addition to monitoring GDPR compliance issues, companies can also expect the EU to publish its long-awaited revised E-Privacy Directive, which governs digital marketing for entities that fall outside of the traditional telecommunications construct.

While companies will spend much of 2019 ensuring that they are in compliance with European mandates, when it comes to the CCPA companies are likely to focus on efforts to amend the law that critics argue was hastily drafted and enacted. Thus, 2019 is likely to be a year in which companies and

privacy advocates work to resolve ambiguities and other contentious elements of the CCPA, including the section 1798.140 definition of "personal information," which critics argue is over broad, and the section 1798.105 private right of action, which companies worry could lead to an endless cycle of lawsuits. While it is possible that we will see certain limited amendments to the California law, companies should not be singularly focused on effectuating legislative change; instead, companies should undertake concerted efforts to ensure that they are in compliance with the CCPA well in advance of the January 1, 2020 effective date.

Beyond California, other American states are likely to consider enacting their own privacy laws. In Washington, for example, State Senator Reuven Carlyle has expressed his intent to introduce comprehensive privacy legislation during the 2019 session. During an event at Seattle University Law School in November 2018, Senator Carlyle indicated that he was still contemplating potential models for the law, including both the GDPR and the CCPA.

The course that individual states pursue with respect to privacy will influence—and be influenced by—the steps that Congress takes in 2019 to enact comprehensive national privacy legislation. While privacy and security are undoubtedly significant priorities for both Democrats and Republicans on the Hill, given the scope of priorities in the new legislative session (as well as residual impacts of the government shutdown), members may be inclined to take a "wait and see" approach and act only if necessary. Of course, if news breaks of yet another massive data breach affecting U.S. citizens, or if multiple states enact potentially conflicting privacy laws that potentially frustrate companies' ability to operate and innovate, then Congress may be forced to take swift action and implement a national law.

Beyond Congress, the Federal Trade Commission ("FTC") also warrants attention in 2019. Specifically, companies should look to see whether the Commission takes a more aggressive enforcement role when it comes to abuses of privacy. While the FTC has shown a willingness to pursue enforcement actions in the data breach context, the Commission has been far less forceful on the privacy side. This difference in approach is largely due to degree of perceived impacts on consumers—with data breach cases creating more immediate and tangible harm to consumers. While to date the FTC has avoided developing any privacy standards beyond its existing section 5 unfair or deceptive acts or practices standard, the Commission has announced a February 2019 hearing to discuss the Commission's remedial authority under section 5 specifically in the context of privacy which signals the agency may be willing to reevaluate the scope and effectiveness of this authority.

More generally, 2019 may see continued action by federal and state legislators and regulators to prescribe industry- or device-specific rules governing IoT, particularly since millions of additional new devices will join the network in the coming months and years.

Van Ness Feldman LLP

Transportation - Autonomous Vehicles

2018 Developments

2018 was a year of both successes and failures for the development and deployment of autonomous vehicles ("AVs"). On the one hand, the automotive industry and Silicon Valley continued to invest tremendous sums of money into this promising and burgeoning technology. However, 2018 was also marked by tragedy and wavering public trust in the technology, as the AV industry witnessed the first pedestrian fatality due to an autonomous vehicle and declining public support for the technology. Collectively, these missteps by the industry have brought the near-term deployment of the technology into question.

Despite those setbacks, both industry and the federal government continue to push forward. In 2018, five technology developers—Nvidia, Starsky Robotics, Uber, Waymo and Zoox—submitted Voluntary Safety Self-Assessments under the reporting framework established in the second iteration of Department of Transportation's ("DOT")AV guidance document from 2017, "A Vision for Safety 2.0." In October 2018, DOT released the third iteration of that guidance, "Preparing for the Future of Transportation: Automated Vehicles 3.0", which seeks to remove barriers to innovation by clarifying the roles of federal agencies affected by automation and making policy pronouncements aimed at facilitating AV deployment (you can read more about the DOT guidance here).

Congress also continued to consider and debate legislation that would have established a mandatory regulatory framework for AVs, though legislation ultimately never reached the President's desk. While House successfully passed AV legislation unanimously in 2017, the Senate's AV START Act stalled over provisions related to safety, liability and federal preemption of state regulatory authorities included in the legislation.

2019 Look Ahead

Notwithstanding the disappointing outcome for AV legislation in 2018, proponents of the legislation in both the House and Senate are likely to revive their efforts to pass an AV bill in a similar form this year. With that said, where it seemed assured that AV legislation would be enacted in 2018, the politics for AVs are far murkier in 2019. The Senate Commerce, Science and Transportation Committee, the committee with jurisdiction over AV legislation, has a new Chairman and Ranking Member whose dedication to passing AV legislation is not clear. In the House, the new Democratic majority may be inclined to make changes to legislation passed with a Republican majority in 2017.

Barring another significant incident or pedestrian fatality during testing, AV development should retain its forward momentum in 2019 as industry continues to invest considerable resources and manpower in

the technology. The current voluntary regulatory environment fostered by DOT also favors further progress, and DOT is still expected to release the fourth version of its AV guidance in the fall.

The Legislative Branch and Cybersecurity

2018 Developments

Cybersecurity issues were at the forefront of the Congressional radar through much of 2018, particularly in the lead-up to the midterm elections. While several legislative initiatives expired at the end of the 115th Congress, lawmakers were able to pass impactful legislation that began to reorient the federal government's response to cybersecurity threats to critical infrastructure, including:

- The Cybersecurity and Infrastructure Agency Act of 2018 (H.R. 3359). The bill renamed the National Protection and Programs Directorate (NPPD) at DHS to the Cybersecurity and Infrastructure Security Agency (CISA). CISA became a standalone federal agency within DHS and serves as the leading civilian cybersecurity agency, with a mission to secure federal networks and U.S. critical infrastructure.
- The John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (H.R. 5515). The NDAA contained several key cybersecurity provisions. The bill establishes U.S. policy on cyber warfare and deterrence, addresses supply chain concerns, facilitates collaboration between the federal government and the private sector, and establishes the Cyberspace Solarium Commission tasked with developing a comprehensive approach to defending the U.S. from significant cyber attacks.
- The FY 2019 Energy-Water Appropriations Act (H.R. 5895). Included in a package of three annual appropriations bills, the Energy-Water spending bill appropriated $120 million in funding for the new Office of Cybersecurity, Energy Security and Emergency Response (CESER) at the Department of Energy. CESER, established by Secretary of Energy Rick Perry in early 2018, will bolster the energy infrastructure security work formerly housed in DOE's Office of Electricity.
- The FY 2018 Consolidated Appropriations Act (H.R. 1625). Signed into law in March 2018, the FY 2018 omnibus spending bill authorized the Election Assistance Commission (EAC) to issue $380 million worth of grants for states to upgrade their election systems in advance of the 2018 midterms. About a third of those grant dollars were spent on cybersecurity improvements.

Already, several pieces of legislation applicable to the energy sector that failed to pass during the 115th Congress have been reintroduced and are pending, including:

- Enhancing Grid Security through Public-Private Partnerships Act (H.R. 359): Directs DOE to facilitate and encourage public-private partnerships in order to improve cybersecurity of electric

utilities. The legislation would improve sharing of best practices and data collection, along with providing training and technical assistance to electric utilities in order to address and mitigate cybersecurity risks.

- Cyber Sense Act (H.R. 360): Creates a voluntary Department of Energy 'Cyber Sense' program that would identify and promote cyber-secure products for use in the bulk-power system. The bill also establishes a testing process for the products along with a reporting process of cybersecurity vulnerabilities
- Energy Emergency Leadership Act (H.R. 362): Requires the Secretary of Energy to assign responsibility for energy emergency and security functions to an assistant secretary.
- Pipeline and LNG Facility Cybersecurity Preparedness Act (H.R. 370): Requires DOE to conduct a program to promote physical security and cybersecurity of natural gas and hazardous liquid pipelines and liquefied natural gas (LNG) facilities.
- Securing Energy Infrastructure Act (H.R. 680 / S. 174): Establishes a two-year program within the National Laboratories to identify cyber vulnerabilities in the energy sector, and to test technologies that could defend the grid against cyber attacks.

2019 Look Ahead

After the midterm elections brought sweeping changes to Washington, the 116th Congress convened in January 2019 with a new Democratic majority in the House of Representatives and, along with it, a new set of priorities for the chamber. The Senate convened with a slightly larger Republican voting majority that may look to act on a slate of bills that did not make it across the finish line in the last Congress. In 2019, we expect Congressional action to address or provide oversight on several major cybersecurity issue areas, including but not limited to:

- Election security;
- Oil and natural gas pipeline cybersecurity;
- Electric grid resilience;
- Privacy;
- Supply chain risks;
- Workforce development;
- Cyber incident response, and;
- Deterrence activities.

With the specter of Presidential election politics looming later this year, it was already difficult to predict with certainty the ability or political will of Congress to pass major legislation in 2019. The ongoing partial federal government shutdown complicates matters even further. Both parties in Congress are reluctant to project a business-as-usual image by turning to other legislative efforts while federal employees are furloughed. With no immediate path to end the shutdown, legislating could remain at a halt for an indefinite period. Critical government cybersecurity functions are ongoing through the shutdown, but policy development, agency hiring, and federal contract work are all significantly affected.

Nonetheless, the leaders of nearly every relevant House and Senate Committees of jurisdiction have promised hearings on cybersecurity issues and mounting threats across domestic critical infrastructure sectors may necessitate swift action from Congress.

CONCLUSION

The vast and varied legislative and policy developments in cybersecurity during 2018 demonstrate that the White House and Congress are committed to building a foundation for additional progress in the fight to protect infrastructure and national security. This momentum will continue in 2019, and the Cybersecurity Team at VNF stands ready to keep its clients informed and at the forefront of these discussions. Please do not hesitate to contact the Van Ness Feldman Cybersecurity Team if you have any questions or need more information.

Gwen Keyes Fleming, Mike Farber, T.C. Richmond, Tracy Nagelbush, Scott Nuzum, Darsh Singh, James Bayot, and Mike Weiner contributed to this report.