COVINGTON

AI and IoT Legislative Developments: First Quarter 2019

May 1, 2019

Artificial Intelligence & the Internet of Things

Federal and state policymakers introduced a range of new measures on artificial intelligence ("AI") and the Internet of Things ("IoT") in the first quarter of 2019. In our initial AI & IoT Quarterly Legislative Update, we detail the notable legislative events from this quarter on AI, IoT, cybersecurity as it relates to AI and IoT, and connected and autonomous vehicles ("CAVs"). Unlike prior years, in which federal lawmakers largely called for studies of these new technologies and supported investments in them, policymakers are increasingly introducing substantive proposals—particularly on AI and cybersecurity, and at the state level.

Artificial Intelligence

Federal lawmakers proposed three notable measures in the first quarter on AI, including a resolution supporting the development of guidelines for the ethical development of AI, introduced by Reps. Brenda Lawrence and Ro Khanna (H. Res. 153). As described on our blog, the resolution calls on the Government to work with stakeholders to ensure that AI is developed in a "safe, responsible, and democratic" fashion. Senators Roy Blunt and Brian Schatz also introduced a measure prohibiting businesses from engaging in certain uses of facial recognition technology; the measure would be enforced by the Federal Trade Commission ("FTC") and state attorneys general (S. 847). In addition, Rep. Darren Soto introduced the Artificial Intelligence Job Opportunities and Background Summary ("AI JOBS") Act of 2019 (H.R. 827), which directs the Secretary of Labor to submit a report to Congress on the impact of AI on the workforce, after collaboration with a range of stakeholders including industry, educational institutions, and other federal agencies.

More recently, on April 10, Senators Ron Wyden and Cory Booker announced the introduction of the Algorithmic Accountability Act of 2019, which would require the FTC to issue regulations requiring certain companies to perform studies evaluating the degree of accuracy, fairness, bias, discrimination, privacy and security in automated decision systems. Specifically, the regulations would require certain companies subject to the FTC's jurisdiction to conduct both: (1) "automated decision impact assessments" of "high-risk automated decision systems" focused on the process for developing the system, including its design and the training data used, and (2) "data protection impact assessments" of "high-risk information systems," evaluating the extent to which those systems protect the privacy and security of personal information they process.

States are also actively considering AI, including its use for government services. In Washington State, a new measure would limit the use of automated decision systems by public agencies (S.B. 5527). In California, two bills would establish a commission to assess how AI and data science could be used to improve state services (A.B. 976), and to report to the state legislature on

minimum standards for the use of AI in state government (A.B. 459). More broadly, another California bill would establish a working group to evaluate the use of AI by California-based businesses and best practices for enabling AI to benefit California businesses and residents (A.B. 1576).

Internet of Things

In the last Congress, lawmakers focused on proposals like the State of Modern Application, Research, and Trends of IoT ("SMART IoT") Act (H.R. 6032), which would direct the Department of Commerce to study the IoT industry, and the Developing Innovation and Growing the Internet of Things ("DIGIT") Act (S. 88), which would direct the Secretary of Commerce to convene a working group to make recommendations and report to Congress on IoT. Neither of those measures was enacted into law. This term, Senators Ed Markey and Josh Hawley introduced a bill to amend the Children's Online Privacy Protection Act ("COPPA"); the proposal would impose cybersecurity requirements for connected devices aimed at children and would require the packaging of such connected devices to contain a "privacy dashboard" describing how personal information is collected, transmitted, retained, used, and protected (S. 748). The Smart Manufacturing Leadership Act, introduced by Rep. Peter Welch, (H.R. 1633) requires the Secretary of Energy to develop a plan for developing smart manufacturing, defined to include among other technologies, advanced sensing and computing technologies that optimize energy efficiency.

At the state level, California has introduced four notable bills on IoT, including the Smart Speaker Privacy Act, which would prohibit a smart speaker from saving or recording verbal commands or requests, as well as conversations (A.B. 1395). California lawmakers are also debating an amendment to the California Minor Erasure Law that would require manufacturers of connected devices directed towards minors to prominently display on the device's packaging a standardized dashboard detailing whether, what, and how personal information of a minor is collected, transmitted, retained, used, and protected (S.B. 299). In addition, California introduced a bill that would allow a state family court to issue an *ex parte* order prohibiting the use of a connected device for harassment (A.B. 455), and a measure to establishing funding for smart cities grants (A.B. 659). Elsewhere, Massachusetts introduced a measure to convene a commission to study the impact on the state's workforce of automation, artificial intelligence, global trade, access to new forms of data, and IoT (S. 210).

Cybersecurity - Relating to AI and IoT

In March, Senators Mark Warner and Cory Gardner re-introduced the IoT Cybersecurity Improvement Act (S. 734), which seeks to leverage the federal Government's procurement power to encourage increased cybersecurity for IoT devices more broadly. As detailed in our blog post, this bill would require the National Institute of Standards and Technology ("NIST") to complete ongoing IoT cybersecurity efforts and to develop recommendations on the appropriate use and management of IoT devices owned or controlled by the federal Government. The Office of Management and Budget ("OMB") would then be required to issue guidelines on using and managing IoT devices for each government agency, based on NIST's recommendations.

A host of other measures aim to shore up cybersecurity in infrastructure and critical infrastructure, including bills addressing cybersecurity in pipelines (H.R. 370, S. 300), the energy grid (S. 174, H.R. 680, H.R. 359, H.R. 360), and transit (S. 846). Concerns about workforce development are

also prompting policymakers to support training a domestic cybersecurity workforce (H.R. 1592, H.R. 334, S. 876) and funding cybersecurity research (H.R. 1062, S. 333, H.R. 542).

At the state level, Virginia in January introduced an IoT cybersecurity measure similar to California's first-in-the nation legislation enacted last year; the measure would require manufactures of connected devices to equip them with reasonable security features (H.B. 2793). Massachusetts lawmakers are also considering a measure that would require the state Office of Consumer Affairs and Business Regulation to issue regulations requiring IoT device makers and autonomous vehicle manufacturers to safeguard personal information (S. 2056).

Connected and Autonomous Vehicles

In the last Congress, lawmakers advanced two measures focused on CAVs: the Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution ("SELF DRIVE") Act (H.R. 3388) and American Vision for Safer Transportation through Advancement of Revolutionary Technologies ("AV START") Act (S. 1885), but neither was enacted into law. Policymakers have indicated that some form of the prior measures may be re-introduced, but they have not yet done so.

In the absence of federal legislation, state policymakers are pushing forward on measures to study or regulate CAVs. In California, one new bill would establish a working group on autonomous passenger vehicle policy development (S.B. 59) while another would require transit operators to ensure certain automated transit vehicles are staffed by employees (S.B. 336). In Washington, a new measure to regulate "personal delivery devices" that deliver property via sidewalks and crosswalks (*e.g.*, wheeled robots) has already passed both houses of the state legislature. In Pennsylvania, which last year passed legislation creating a commission on "highly automated vehicles," a new proposal would authorize the use of an autonomous shuttle vehicle on a route approved by the Pennsylvania Department of Transportation (H.B. 1078).

This is the first installment in Covington's quarterly update on AI and IoT legislative developments.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Artificial Intelligence and Internet of Things initatives:

Layth Elhassani	+1 202 662 5063	lelhassani@cov.com
Holly Fechner	+1 202 662 5475	hfechner@cov.com
Muftiah McCartin	+1 202 662 5510	mmccartin@cov.com
Lindsey Tonsager	+1 415 591 7061	ltonsager@cov.com
Kate Goodloe	+1 202 662 5505	kgoodloe@cov.com