COVINGTON

AI and IoT Legislative Developments: Third Quarter 2019

October 21, 2019

Artificial Intelligence and Internet of Things

Federal policymakers continued to focus on artificial intelligence ("AI") and the Internet of Things ("IoT") in the second quarter of 2019, including by introducing substantive bills that would regulate the use of such technology and by supporting bills aimed at further study of how such technology may impact different sectors. In our third 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").

Artificial Intelligence

Members in both the House and Senate introduced legislation focused on researching generative adversarial networks—the technology behind "deepfakes." Theses new bills follow a hearing in June 2019 by the House Permanent Select Committee on Intelligence on the national security challenges of artificial intelligence, manipulated media, and deepfake technology.

- Rep. Anthony Gonzalez (R-OH) introduced the **Identifying Outputs of Generative Adversarial Networks ("IOGAN") Act** (H.R. 4355), which would direct both the National Science Foundation and the National Institute of Standards and Technology ("NIST") to support research on deepfakes, and to issue a joint report regarding research opportunities with the private sector.

- Sen. Rob Portman (R-OH) introduced the **Deepfake Report Act of 2019** (S. 2065), which would require the Department of Homeland Security to produce annual reports for the next five years on the state of "digital content forgery" technology. The bill defines "digital content forgery" as "the use of emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead."

Internet of Things

Lawmakers have also focused on connected devices in the home, introducing bills that would grant the Federal Trade Commission ("FTC") broader authority to regulate these devices. Although the definitions of connected devices are not consistent, these bills generally include smart home speakers and home assistants. Two proposals focus specifically on smart home devices' recording capabilities:

- Sen. Cory Gardner (R-CO) introduced the **Protecting Privacy in our Homes Act** (S. 2532). The bill would require the FTC to promulgate rules requiring manufacturers of internet-connected devices to provide notice "on the packaging" of a device when it contains a camera or microphone, but is not marketed as such, and would make a violation of these rules an unfair or deceptive act or practice. Covered devices are defined to include internet-connected devices, a component of which is a camera or microphone, but that are not specifically marketed as a camera or microphone.

- Rep. Seth Moulton (D-MA) introduced the **Automatic Listening Exploitation ("ALEXA") Act of 2019** (H.R. 4048). The bill would allow the FTC and state attorneys general to bring actions against smart speaker and video doorbell manufacturers when such devices record the private conversations of users who have not said the device's "wake word" (e.g., "Alexa," "Hey Google," "Hey Siri," etc.) or otherwise activated the device. (Such an action would be an unfair or deceptive act or practice.) The bill authorizes penalties of up to $40,000 per infraction. It would create data subject rights, providing consumers with the right to have their recordings, transcripts, and videos deleted. "Smart speaker" is defined as an internet-enabled electronic device that can be controlled through a voice-user interface and that provides a smart speaker service to a user. "Video doorbell" as an internet-enabled doorbell, equipped with a camera or microphone, or both, that notifies a user when a guest arrives, is activated at the press of a button, and which may allow the user to watch or talk to the guest through the doorbell.

Cybersecurity – Relating to AI and IoT

Lawmakers continued to focus their attention on bills relating to energy, infrastructure, and supply chain issues. Committees in both chambers held mark-up session for bills previously introduced, including the **Pipeline Security Act** (H.R. 3699), the **Enhancing Grid Security through Public-Private Partnerships Act** (H.R. 359), the **Cybersecurity Preparedness Act** (H.R. 370), the **Cyber Sense Act of 2019** (H.R. 360), and the **Enhancing Grid Security through Public-Private Partnership Act** (S. 2095). Each of these bills was subsequently ordered to be reported by the House Homeland Security and Energy & Commerce Committees, and the Senate Energy & Natural Resources Committee, respectively.

Additionally the following bills were introduced in the same area during the third quarter:

- **Next Generation Electric Systems Act of 2019** (S. 2380): This bill directs the Secretary of Energy to establish a grant program for the transformation of the electric grid. Eligible projects must include development of a cybersecurity plan that is written in accordance with guidelines developed by the Secretary of Energy.

- **Energy Cybersecurity Act of 2019** (S. 2333) - This bill would expand energy sector operation support for the cyberresilience program and require the development of modeling related to assessing energy infrastructure risk, including due to cyber threats.

- **Grid Modernization Act** (S. 2332) - This bill would modernize the electric grid, including by developing physical and cybersecurity plans to secure the grid.

- **Manufacturing, Investment, and Controls Review for Computer Hardware, Intellectual Property, and Supply ("MICROCHIPS") Act of 2019** (S. 2316) - This bill would require the submission of a plan for strengthening the supply chain intelligence function and creation of the National Supply Chain Intelligence Center within the Office of the Director of National Intelligence.

The **IoT Cybersecurity Improvement Act** (S. 734), which was introduced by Senators Mark Warner (D-VA) and Cory Gardner (R-CO) earlier this year, advanced through Committee with an amendment as reported on in our last quarterly update. A committee report of the bill was also released and included the Congressional Budget Office's implementation cost estimate: $35 million over the 2019-2024 time period.

Connected and Autonomous Vehicles

Federal lawmakers continued to demonstrate interest in a comprehensive CAV bill—for example, at the end of July the House Energy and Commerce Committee and Senate Commerce Committee sought stakeholder input with a stated intention of informing a bipartisan and bicameral CAV bill—but legislation has yet to emerge.

In the absence of a comprehensive proposal, federal lawmakers have introduced bills that target the wider automotive sector but are relevant to CAVs. Sen. Ed Markey (D-MA) introduced the **Security and Privacy in Your Car ("SPY Car") Act** of 2019 (S. 2182), which is designed to protect consumers from security and privacy threats to their motor vehicles. Sen. John Barrasso (R-WY) introduced **America's Transportation Infrastructure Act of 2019** (S. 2302), which provides the largest amount of funding for highway reauthorization legislation in history and specifically includes a section on an emerging technology research pilot program. The bill would also require the Federal Highway Administration to develop a tool to assist transportation authorities in handling cyber incidents, and to designate a "cyber coordinator" office.

Federal regulators also continued to take an interest in the CAV sector. For example, the National Highway Traffic Safety Administration ("NHTSA") continues to consider comments on petitions from two industry stakeholders, General Motors and Nuro, regarding exemptions from the Federal Motor Vehicle Safety Standards in connection with automated vehicles. NHTSA additionally sought comments on the Federal Motor Carrier Safety Regulations (*i.e.*, the regulations governing commercial motor vehicles such as trucks), which may be a barrier to deploying certain automated driving systems ("ADS") on the road. Furthermore, in the third quarter the Department of Transportation ("DOT") announced nearly $60 million in federal grant funding to eight projects in seven states to test the safe integration of ADS on national roadways.

This is the third installment of 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 Communications and Media practice:

Muftiah McCartin	+1 202 662 5510	mmccartin@cov.com
Layth Elhassani	+1 202 662 5063	lelhassani@cov.com
Holly Fechner	+1 202 662 5475	hfechner@cov.com
Jennifer Johnson	+1 202 662 5552	jjohnson@cov.com
Lindsey Tonsager	+1 415 591 7061	ltonsager@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.