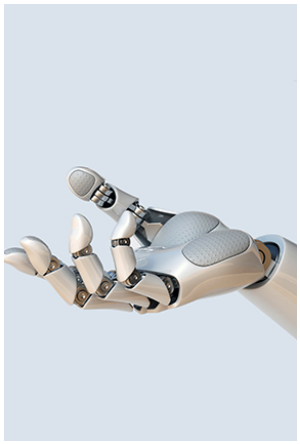
Van Ness Feldman LLP
vnf.com



Emerging Technologies Update

FEBRUARY 26, 2019

R. Scott Nuzum, Eric Wagner, Maranda Compton, and Michael Weiner

In this edition of the Emerging Technologies Update:

- **Analysis on OpenAI's announcement of an artificial intelligence (AI) model capable of independently writing text, including why companies, governments, and individuals should be paying attention.**
- **Overview and analysis of President Trump's February 11, 2019 Executive Order on AI.**
- **A chart detailing other executive branch actions taken in the past month that may impact emerging technologies.**
- **Highlights of notable legislative branch developments, including the potential for renewed congressional activity on autonomous vehicles (AVs).**

In the News

On February 14, 2019, OpenAI—a nonprofit AI research company—revealed that it had developed an AI model called GPT-2 "which generates coherent paragraphs of text, achieves state-of-the-art performance on many language modeling benchmarks, and performs rudimentary reading comprehension, machine translation, question answering, and summarization—all without task-specific training." While the performance of GPT-2 itself was notable, it was equally telling that Open AI made a decision not to publish their underlying model out of fear for potential misuse.

GPT-2 is the latest development in synthetic content—online video, audio, or textual content that appears authentic, but is actually computer generated. To date, focus has centered on "deepfakes"—videos that utilize deep learning AI to create content that looks convincingly real but which are, in fact, fabricated. One early and widely-circulated example of the potential capabilities of deepfake videos to deceive showed former President Barack Obama warning against the threat of deepfakes. GPT-2 represents a new type of synthetic content—the program is a text generator whereby the AI model is given sample text and then utilizes predictive analytics to independently draft more text. While the quality of GPT-2-generated text varies, it will not be long before the program (or something similar) produces text that is indistinguishable from a human writer.

So why should any of this matter to companies, governments, and individuals? First, text generating AI like GPT-2 will in the near-future present the opportunity to generate content—press releases, reports, legal briefs, social media posts—quickly and at lower cost. Certainly, quality control will remain an issue, but the potential efficiencies and cost savings associated with AI-enabled text generators will justify their use.

Beyond the beneficial uses, though, companies, governments, and individuals must also start thinking about potentially nefarious applications of this type of software and other synthetic content, including deepfakes. In articulating its reasons for withholding public release the GPT-2 code, OpenAI specifically cited the high risk of malicious uses. And while we should applaud OpenAI for exercising discretion in this instance, it is also important to recognize that OpenAI is not the only entity working on predictive text-generators—it is increasingly likely that a GPT-2-type tool will be available in the near future.

Once these tools are publicly available, it is not difficult to see how AI-enabled text generators could be used for destructive purposes. For example, bad actors could use a program like GPT-2 to generate spam, misinformation, or negative product reviews to annoy, overwhelm, or otherwise harm individuals, companies, and governments. In the most extreme cases, a well-timed deepfake or AI-generated press release could be deployed to influence an election or to tank a particular stock. And while it may ultimately be possible to disprove the authenticity of this type of content, doing so will take time.

Taking into account the viral nature of the internet—and the speed at which information (or disinformation) spreads—it is possible that a deepfake would generate economic or political harm in a nearly instantaneous manner, making damage control efforts all but impossible.

Given the potential for negative impacts arising from synthetic content, governments, companies, and individuals should undertake active measures to mitigate likely impacts. To this end, a company should develop a response plan that enables swift and decisive action the moment a deepfake is released. As part of the response process, companies should engage in tabletop exercises, war games, and other simulations that allow individuals to test the effectiveness of response plans (much in the same manner that they do for a potential data breach or other cyber-incident). In addition, governments, companies, and individuals should make certain that they understand if and how the failure to adequately police and respond to a deepfake might create potential legal liability.

Van Ness Feldman's cybersecurity practice group is available to help entities seeking to scope appropriate synthetic content response strategies.

Executive Branch Actions

President Trump Issues Artificial Intelligence Executive Order

On February 11, 2019, the White House released Executive Order (EO) 13859, "Maintaining American Leadership in Artificial Intelligence." The EO constitutes the most definitive acknowledgement yet by the Trump Administration of AI's present and future significance, recognizing the inherent promise of AI "to drive growth of the United States economy, enhance our economic and national security, and improve our quality of life." The EO also highlights the status of the United States as a global leader in AI research and development (R&D) and deployment. Importantly, the EO demonstrates that the Administration understands that AI is a critical element in economic and national security and that the United States plays an important role "in facilitating AI R&D, promoting the trust of the American people in the development and deployment of AI-related technologies, training a workforce capable of using AI in their occupations, and protecting the American AI technology base from attempted acquisition by strategic competitors and adversarial nations."

The EO outlines an "American AI Initiative" guided by five principles:

1. The United States must drive technological breakthroughs in AI across the Federal Government, industry, and academia in order to promote scientific discovery, economic competitiveness, and national security.

2. The United States must drive development of appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies in order to enable the creation of new AI-related industries and the adoption of AI by today's industries.

3. The United States must train current and future generations of American workers with the skills to develop and apply AI technologies to prepare them for today's economy and jobs of the future.

4. The United States must foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application in order to fully realize the potential of AI technologies for the American people.

5. The United States must promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations.

The EO is first and foremost a response to China's ambitions (and strategic plan) to become the global leader in AI by 2030. But while China has outlined an actionable strategic plan, the Trump EO is less a strategy document and more an entreaty of general intentions, aimed at reasserting U.S. desires to

remain the global AI leader. Nevertheless, the EO does outline several specific mandates for federal agencies. Among other requirements, the EO directs the heads of all federal agencies to "review their Federal data and models to identify opportunities to increase access and use by the greater non-Federal AI research community in a manner that benefits that community, while protecting safety, security, privacy, and confidentiality." In particular, the EO directs federal agencies to "improve data and model inventory documentation to enable discovery and usability, and [to] prioritize improvements to access and quality of AI data and models based on the AI research community's user feedback."

Additionally, the EO directs the Director of the Office of Management and Budget (OMB), with support from other officials, to issue a memorandum to the heads of all agencies that (i) "inform[s] the development of regulatory and non-regulatory approaches by such agencies regarding technologies and industrial sectors that are either empowered or enabled by AI and advance American innovation;" and (ii) "consider[s] ways to reduce barriers to the use of AI." In order to secure public trust in the development and implementation of AI applications, the EO directs OMB to issue a draft of the memorandum for public comment before it is finalized.

The EO also charges the Secretary of Commerce, through the Director of the National Institute of Standards and Technology (NIST), with the development of a "plan for federal engagement in the development of technical standard and related tools in support of reliable, robust, and trustworthy systems that use AI technologies."

Other Executive Branch Actions

Agency	Action	Notes
Department of Defense (DoD)	Defense Innovation Board; Notice of Federal Advisory Committee Meeting	Public meeting scheduled for **March 21, 2019** from 9:30 am to 12:30 pm; agenda includes discussion of development of principles for the ethical use of AI and the viability of 5G capability for DoD
DoD	"Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity."	Outlines four "strategic focus areas:" (i) Delivering AI-enabled capabilities that address key missions; (ii) Partnering with leading private sector technology companies, academia, and global allies and partners; (iii) Cultivating a leading AI workforce; and (iv) Leading in military ethics and AI safety.
Federal Aviation Administration (FAA)	Operation of Small Unmanned Aircraft Systems Over People; Notice of Proposed Rulemaking	For more information see January 23, 2019 Emerging Technologies Update; public comments due by **April 15, 2019**
FAA	Safe and Secure Operations of Small Unmanned Aircraft Systems; Advanced Notice of Proposed Rulemaking	For more information see January 23, 2019 Emerging Technologies Update; public comments due by **April 15, 2019**
Federal Communications Commission (FCC)	Use of Spectrum Bands Above 24 GHz for Mobile Radio Service; Final Rule	Action is part of FCC's effort to make spectrum available for 5G wireless, IoT, and other innovative services; effective **March 7, 2019**
NIST	Draft Security for IoT Sensor Networks: Building Management Systems Case Study	NIST's National Cybersecurity Center of Excellence (NCCoE) is exploring common components of sensor networks and the associated security requirements of those components for the secure functioning of the IoT sensor network; NIST is seeking feedback through **March 18, 2019**

National Science Foundation (NSF)	Request for Information: Action on Interoperability of Medical Devices, Data, and Platforms to Enhance Patient Care	NSF's Networking and Information Technology Research and Development National Coordinations Office seeks input on new approaches from industry, academia, and non-governmental organizations to solve interoperability issues between medical devices, data, and platforms; comment period closes **March 15, 2019**
Department of State	Notice of Public Meeting to prepare for 106 session of the International Maritime Organization's Legal Committee	Meeting to be held on **March 20, 2019**; agenda includes discussion of a regulatory scoping exercise and gap analysis of conventions emanating from the Legal Committee with respect to Maritime Autonomous Surface Ships (MASS)

Legislative Branch Actions

Congress Seeks to Resume Push for Autonomous Vehicle Legislation

On February 14, Senator John Thune (R-SD) indicated that he is working with Senator Gary Peters (D-MI) to reintroduce a new version of the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act, which failed to pass the Senate last year. The bill—introduced in the 115th Congress as S.1885—passed out of the Senate Commerce, Science and Transportation Committee last year before being held up over safety and liability concerns.

With the start of the 116th Congress, AV legislation faces new challenges. First, Senator Thune no longer chairs the Commerce Committee and, therefore, does not control the Committee's legislative agenda. Second, the Democratically-led House of Representatives may choose to make changes to the House-passed bill, the Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution (SELF DRIVE) Act, which passed in 2017.

Despite these challenges, the fact that Senators Thune and Peters continue to show interest in reintroducing and moving the legislation is a notable development for the AV industry this early in the new Congress.

Other Legislative Branch Actions

Title	Sponsor	Notes
H.R. 763 – Energy Innovation and Carbon Dividend Act of 2019	Rep. Theodore Deutch (D-FL-22)	Introduced Jan. 24, 2019; would create a "Carbon Dividend Trust Fund" in order to encourage market-driven innovation of clean energy technologies and market efficiencies.
H.R. 827 – AI JOBS Act of 2019	Rep. Darren Soto (D-FL-9)	Introduced Jan. 28, 2019; would require the Secretary of Labor to prepare a report on AI and its impact to the workforce; report would identify industries that are projected to have the most growth in AI use and determine whether the technology will result in the enhancement of workers' capabilities or their replacement.

Van Ness Feldman LLP
vnf.com

S.384 – A bill to require the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, to help facilitate the adoption of composite technology in infrastructure in the United States, and for other purposes	Sen. Shelley Moor Capito (R-WV)	Directs NIST to implement the recommendations of the December, 2017 report entitled "Road Mapping Workshop Report on Overcoming Barriers to Adoption of Composites in Sustainable Infrastructure"; directs NIST to conduct pilot program to assess feasibility and advisability of adopting composite technology in sustainable infrastructure.
S. 404 – A bill to require the Commissioner of the U.S. Customs and Border Protection to acquire and enhance technology and assets in rural and remote areas near the southern border and to establish and Agent Mobility Demonstration Program	Sen. Marin Heinrich (D-NM)	As of February 26, 2019, bill text is not available

For more information

Van Ness Feldman's Technology Regulation and Policy team is available to provide counsel to entities as they assess the implications of any of the proposed federal actions identified in this update. Should you have any questions, please contact the authors of this update.

Follow us on Twitter @VanNessFeldman and @rsnuzum