

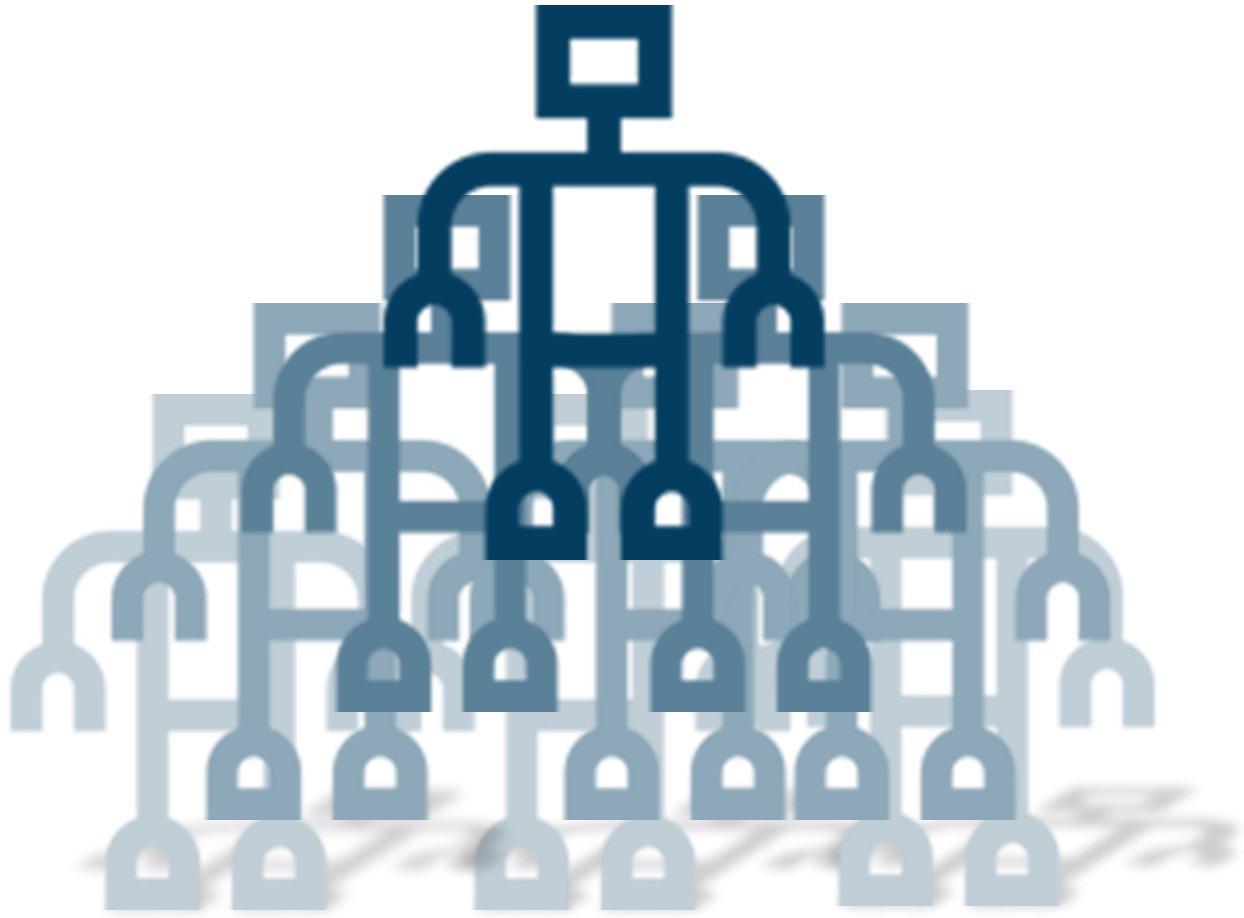
CORD

Rise of the Machines: Artificial Intelligence and its Growing Impact on U.S. Policy

Item Type	House Bipartisan Staff Report
Download date	2025-03-27 16:52:14
Link to Item	https://hdl.handle.net/20.500.14300/2398

Rise of the Machines

Artificial Intelligence and its Growing Impact on U.S. Policy
Chairman Will Hurd and Ranking Member Robin Kelly



Subcommittee on Information Technology
Committee on Oversight and Government Reform
U.S. House of Representatives
September 2018

EXECUTIVE SUMMARY

Beginning in February of 2018, the Subcommittee on Information Technology of the House Committee on Oversight and Government Reform held a series of hearings on artificial intelligence (AI). In connection with those hearings, majority and minority staff met jointly with experts from academia, industry, and government, and reviewed multiple reports from leading AI experts.

Through these efforts, several points became evident. First, AI is an immature technology; its abilities in many areas are still relatively new. Second, the workforce is affected by AI; whether that effect is positive, negative, or neutral remains to be seen. Third, AI requires massive amounts of data, which may invade privacy or perpetuate bias, even when using data for good purposes. Finally, AI has the potential to disrupt every sector of society in both anticipated and unanticipated ways. In light of that potential for disruption, it's critical that the federal government address the different challenges posed by AI, including its current and future applications. The following paper presents lessons learned from the Subcommittee's oversight and hearings on AI and sets forth recommendations for moving forward.

Underlying these recommendations is the recognition the United States cannot maintain its global leadership in AI absent political leadership from Congress and the Executive Branch. Therefore, the Subcommittee recommends increased engagement on AI by Congress and the Administration.

Chief among the Subcommittee's recommendations is for the federal government to increase federal spending on research and development to maintain American leadership with respect to AI. In response to concerns about AI's potential economic impact, federal, state, and local agencies are encouraged to engage more with stakeholders on the development of effective strategies for improving the education, training, and reskilling of American workers to be more competitive in an AI-driven economy. The Subcommittee further recommends the federal government lead by example by investing more in education and training programs that would allow for its current and future workforce to gain necessary AI skills.

In response to concerns about privacy, the Subcommittee recommends federal agencies review federal privacy laws and regulations to determine how they may already apply to AI technologies within their jurisdiction, and, where necessary, update existing regulations to account for the addition of AI. To account for potential biases in AI systems, federal, state, and local agencies that use AI systems to make consequential decisions about people should ensure that the algorithms that support these systems are accountable and inspectable.

Finally, any regulatory approach to AI should consider whether the risks to public safety or consumers already fall within any existing regulatory frameworks and, if so, whether those existing frameworks can adequately address the risks. Where a risk falls outside an existing regulatory framework, an approach should consider whether modifications or additions are needed to better account for the addition of AI.

As AI technology continues to advance, its progress has the potential to dramatically reshape the nation's economic growth and welfare. It is critical the federal government build upon, and increase, its capacity to understand, develop, and manage the risks associated with this technology's increased use.

INTRODUCTION

Defining AI

This paper defines AI as computational technology that works and reacts in humanlike ways. AI generally falls into two categories: “narrow AI” and “general AI.” Narrow AI addresses or solves specific tasks, “such as playing strategic games, language translation, self-driving vehicles, and image recognition.”¹ General AI, on the other hand, can accomplish more than one task and can move between these tasks based on reasoning.² Witnesses who testified before the Subcommittee suggested that while narrow AI is commonly utilized today, “more general systems . . . that can work across multiple tasks” are underdeveloped at this time.³ The examples of AI that are referred to in this paper concern the field of narrow AI.

Brief Background on AI

The idea of AI first emerged in 1950 with “Computing Machinery and Intelligence,” Alan Turing’s seminal paper addressing the question of whether machines can think.⁴ Turing’s paper also set forth a test for answering this question, and highlighted the issue of whether machines could be developed to learn from experiences similar to the way people do.⁵ The term “artificial intelligence” was later coined in 1956 by John McCarthy after holding the first academic conference on the topic.⁶ The last ten years have seen the most significant developments in AI, largely due to advancements in computing power and increased access to data.

Current Uses of AI

While AI is most closely associated with Silicon Valley and Hollywood, various industries have already deployed the technology. For example, AI is now used in connection

¹ EXECUTIVE OFFICE OF THE PRESIDENT, NATIONAL SCIENCE AND TECHNOLOGY COUNCIL COMMITTEE ON TECHNOLOGY, *Preparing for the Future of Artificial Intelligence*, (Oct. 2016), *online at* https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. *see also* GOVERNMENT ACCOUNTABILITY OFFICE, *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications* (GAO-18-142S) (March 2018), *online at* <https://www.gao.gov/assets/700/690910.pdf>.

² *Id.*

³ *Game Changers: Artificial Intelligence Part 1: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Oren Etzioni, CEO, Allen Institute for Artificial Intelligence)

⁴ Alan M. Turing, *Computing Machinery and Intelligence*, 49 *Mind* 433-460 (1950), *online at* <https://www.csee.umbc.edu/courses/471/papers/turing.pdf> (last accessed Sept. 14, 2018).

⁵ *Id.*

⁶ Gil Press, *Artificial Intelligence Defined as a New Research Discipline: This Week in Tech History*, FORBES (Aug. 28, 2016) *online at* <https://www.forbes.com/sites/gilpress/2016/08/28/artificial-intelligence-defined-as-a-new-research-discipline-this-week-in-tech-history/#6913216e6dd1>.

with mapping applications or “apps” on mobile phones,⁷ tax preparation,⁸ song writing,⁹ and digital advertising.¹⁰ It is also being used in video games and movies to create special effects.¹¹ More recently, the Food and Drug Administration approved an AI algorithm that aids radiologists in detecting wrist fractures.¹² The State of Ohio uses robotics in the Bureau of Criminal Investigation laboratories to help reduce the turnaround time on untested rape kits.¹³ The application of AI facilitated the state testing 14,000 previously untested rape kits and identifying 300 serial rapists linked to 1,100 crimes.¹⁴

While today’s AI products and applications are largely limited to solving specific, discrete tasks, because of its current and potential benefits, AI has generated broad interest across the economy, and as a result, will likely be a key driver of future economic growth and progress.

IMPORTANCE OF U.S. LEADERSHIP IN AI

The United States has traditionally led the world in the development and application of AI-driven technologies.¹⁵ This is due in part to the government’s prior commitment to investing heavily in research and development (R&D) that has, in turn, helped support AI’s growth and development. In 2015, for example, the United States led the world in total gross domestic R&D expenditures, spending \$497 billion.¹⁶

The Subcommittee’s hearings, however, highlighted the fact that the United States’ leadership in AI is no longer guaranteed. During the hearings, several of the witnesses testified

⁷ Nick Statt, *AI is Google’s secret weapon for remaking its oldest and most popular apps*, THE VERGE (May 10, 2018), online at <https://www.theverge.com/2018/5/10/17340004/google-ai-maps-news-secret-weapon-remaking-old-apps-products-io-2018>.

⁸ Adelyn Zhou, *EY, Deloitte, and PwC Embrace Artificial Intelligence For Tax and Accounting*, FORBES (Nov. 14, 2017), online at <https://www.forbes.com/sites/adelynzhou/2017/11/14/ey-deloitte-and-pwc-embrace-artificial-intelligence-for-tax-and-accounting/#2ad76d253498>.

⁹ Matt Jancer, *More Artists are Writing Songs in the Key of AI*, WIRED (May 17, 2018), online at <https://www.wired.com/story/music-written-by-artificial-intelligence/>.

¹⁰ Tom Simonite, *Google and Microsoft Can Use AI to Extract Many More Ad Dollars from Our Clicks*, FORBES (Aug. 31, 2017), online at <https://www.wired.com/story/big-tech-can-use-ai-to-extract-many-more-ad-dollars-from-our-clicks/>.

¹¹ Cade Metz, *Lights, Camera, Artificial Action: Start-Up is Taking A.I. to the Movies*, NEW YORK TIMES (March 26, 2018), online at <https://www.nytimes.com/2018/03/26/technology/artificial-intelligence-hollywood.html>.

¹² FOOD AND DRUG ADMINISTRATION, *FDA permits marketing of artificial intelligence algorithm for aiding providers in detecting wrist fractures* (May 24, 2018), online at <https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm608833.htm>.

¹³ OHIO OFFICE OF THE ATTORNEY GENERAL, Law Enforcement, Bureau of Criminal Investigations, Laboratory Division, (online at <https://www.ohioattorneygeneral.gov/Law-Enforcement/Bureau-of-Criminal-Investigation/Laboratory-Division>), (last visited August 22, 2018).

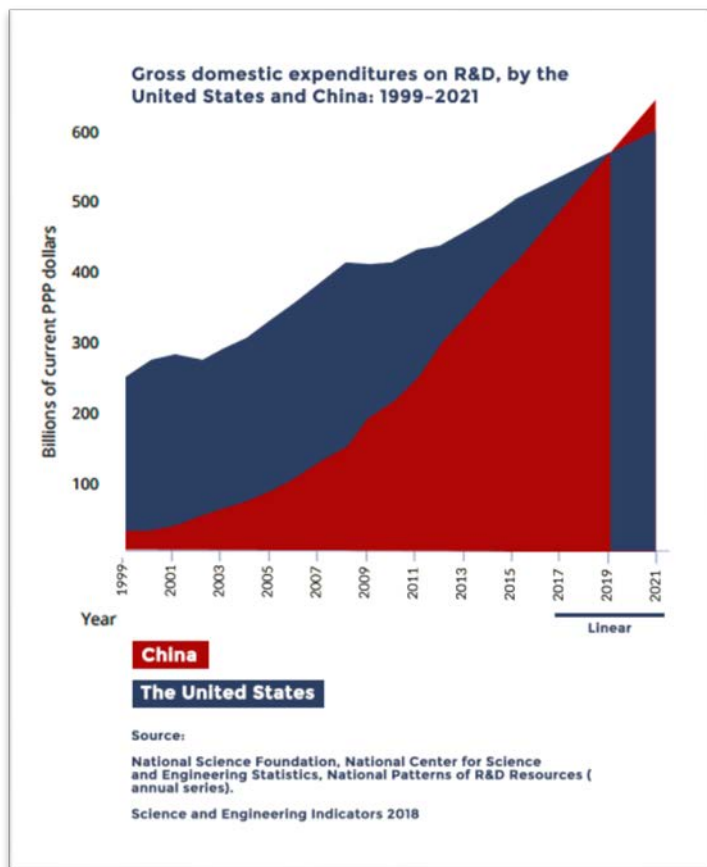
¹⁴ Anna Boiko-Weyrauch, *Her Rapist was Convicted because of a Rape Kit. So Why are So Many Untested?*, KUOW (August 15, 2018) online at <http://kuow.drupal.publicbroadcasting.net/post/her-rapist-was-convicted-because-rape-kit-so-why-are-so-many-kits-untested>.

¹⁵ McKinsey Global Institute, *Artificial Intelligence: Implications for China* (April 2017) online at <https://www.mckinsey.com/~media/McKinsey/Featured%20Insights/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx>.

¹⁶ NATIONAL SCIENCE BOARD, 2018 SCIENCE & ENGINEERING INDICATORS (2018), online at www.nsf.gov/statistics/2018/nsb20181/assets/nsb20181.pdf.

the United States needs to increase its R&D spending to remain competitive in the field of AI. One witness stated, “[w]hile other governments are aggressively raising their research funding, U.S. government research has been relatively flat.”¹⁷

Another witness expressly warned, “[c]urrent federal funding levels are not keeping pace with the rest of the industrialized world.”¹⁸



Notably, China’s commitment to funding R&D has been growing sharply, up 200 percent from 2000 to 2015.¹⁹ On February 7, 2018, the National Science Board’s (Board) and the National Science Foundation’s (NSF) Director, who jointly head NSF, said in a statement that if current trends continue, the Board expects “China to pass the United States in R&D investments” by the end of 2018.²⁰

Recent progress was made when the Defense Advanced Research Projects Agency (DARPA) announced the creation of the Artificial Intelligence Exploration program, “AI Next,” to bolster the United States’ leadership in AI. DARPA plans to invest more than \$2 billion into this program and other existing programs. The program focuses research on “‘third wave’ AI theory and application that will make it possible for

machines to contextually adapt to changing situations.”²¹

¹⁷ *Game Changers: Artificial Intelligence Part 1: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Ian Buck, Vice President and General Manager, Tesla Data Center Business, NVIDIA).

¹⁸ *Game Changers: Artificial Intelligence Part 1: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Amir Khosrowshahi, Vice President and Chief Technology Officer, Artificial Intelligence Group, Intel Corp.).

¹⁹ NATIONAL SCIENCE BOARD, 2018 SCIENCE & ENGINEERING INDICATORS (*online at* www.nsf.gov/statistics/2018/nsb20181/assets/nsb20181.pdf).

²⁰ NATIONAL SCIENCE FOUNDATION, NATIONAL SCIENCE BOARD STATEMENT ON GLOBAL RESEARCH AND DEVELOPMENT (R&D) INVESTMENTS NSB-2018-9 (Feb. 7, 2018), *online at* www.nsf.gov/nsb/news/news_summ.jsp?cntn_id=244465 (last accessed September 17, 2018).

²¹ Defense Advanced Research Projects Agency, *DARPA Announces \$2 Billion Campaign to Develop Next Wave of AI Technologies* (Sept. 7, 2018), *online at* <https://www.darpa.mil/news-events/2018-09-07>.

The chart on the previous page shows China’s rapidly growing investment in AI. Particularly concerning is the prospect of an authoritarian country, such as Russia or China, overtaking the United States in AI. As the Subcommittee’s hearings showed, AI is likely to have a significant impact in cybersecurity, and American competitiveness in AI will be critical to ensuring the United States does not lose any decisive cybersecurity advantage to other nation-states.²²

The loss of American leadership in AI could also pose a risk to ensuring any potential use of AI in weapons systems by nation-states comports with international humanitarian laws. In general, authoritarian regimes like Russia and China have not been focused on the ethical implications of AI in warfare, and will likely not have guidelines against more bellicose uses of AI, such as in autonomous weapons systems.²³

The United States’ competitiveness in AI is also critical to its economic security, as AI is poised to be a key driver of economic growth. AI applications promise to make industry more efficient—cutting down costs, limiting the use of natural resources, and improving the use of finite resources such as “the increasingly crowded electromagnetic spectrum.”²⁴

For example, the Government Services Administration has a robotic processing automation (RPA) pilot that automates portions of the Multiple Award Schedules new offer review process. Presently, contract officers must go through a tedious administrative process, reading through dozens of pages of documentation across multiple IT systems to ensure a vendor’s new offer is consistent with information already in government databases. RPA software offers the capability to perform these tasks, so the contract officers can spend more time engaging with customers.²⁵

In an effort to keep the United States at the forefront of AI developments and advancements, the Obama Administration released three reports in 2016 that assessed the state of AI. The reports focused on the public policy questions AI raises for the country, and proposed a series of recommendations.²⁶ The current Administration should prioritize building on these

²² *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Ben Buchanan, Postdoctoral Fellow, Belfer Center Cyber Security Project, Science, Technology, and Public Policy Program, Harvard University). Dr. Buchanan currently serves as an Assistant Teaching Professor at Georgetown University’s School of Foreign Service.

²³ CENTER FOR A NEW AMERICAN SECURITY, *Autonomous Weapons* (online at <https://www.cnas.org/research/technology-and-national-security/autonomous-weapons>) (accessed June 19, 2018).

²⁴ Spectrum Collaboration Challenge, *What is the Spectrum Collaboration Challenge?* DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, (available at <https://spectrumcollaborationchallenge.com/about/>) (accessed Aug. 15, 2018).

²⁵ *Game Changers: Artificial Intelligence Part II, Artificial Intelligence and the Federal Government: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Mr. Keith Nakasone, Deputy Assistant Commissioner Category Acquisition Management, U.S. General Services Administration).

²⁶ EXECUTIVE OFFICE OF THE PRESIDENT, NATIONAL SCIENCE AND TECHNOLOGY COUNCIL COMMITTEE ON TECHNOLOGY, *Preparing for the Future of Artificial Intelligence*, (Oct. 2016), online at https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_

efforts and ensure federal agencies are implementing these recommendations. Recent efforts by the Trump Administration recognize AI's growing importance. In particular, the Administration has highlighted AI in the 2017 National Security Strategy, 2018 Summary of the National Defense Strategy, the Office of Management and Budget (OMB) and Office of Science and Technology Policy's (OSTP) FY2019 Administration Research and Development Budget Priorities, and the FY2019 Budget Request. OSTP also held a summit on the topic in May 2018, and established the National Science and Technology Council Select Committee on AI.²⁷

As the United States considers the impact of AI in both foreign and economic affairs, we must keep in mind that American values—the right to privacy, free speech, the rule of law, and respect for intellectual property—give America many intangible advantages over other nations. As Subcommittee Chairman Hurd said in June, “the United States boasts a creative, risk-taking culture that is inextricably linked to its free enterprise system.”²⁸ Gary Shapiro testified before the Subcommittee, “[the United States’] competitive strength is innovation.”²⁹ Throughout the hearings, witnesses repeatedly acknowledged these advantages are important components driving American leadership in AI's development and deployment. We cannot presume that these values will automatically secure our leadership, but we should be aware of them and regard them as strengths.

AI'S CHALLENGES

The Subcommittee's hearings showed AI faces a number of different challenges. In this paper, we will address the four challenges discussed during the hearings—workforce, privacy, bias, and malicious use of AI.

Workforce

One of the central concerns raised during the hearings is that AI advancement in the short-term could lead to the loss of jobs due to AI-driven automation.³⁰ A December 2017 report

future_of_ai.pdf; EXECUTIVE OFFICE OF THE PRESIDENT, NATIONAL SCIENCE AND TECHNOLOGY COUNCIL COMMITTEE ON TECHNOLOGY, NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT SUBCOMMITTEE, *The National Artificial Intelligence Research and Development Strategic Plan* (Oct. 2016) *online at* https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf; EXECUTIVE OFFICE OF THE PRESIDENT, *Artificial Intelligence, Automation, and the Economy* (Dec. 2016) *online at* <https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF>.

²⁷ EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF SCIENCE AND TECHNOLOGY POLICY, SUMMARY OF THE 2018 WHITE HOUSE SUMMIT ON ARTIFICIAL INTELLIGENCE FOR AMERICAN INDUSTRY (2018), *online at* <https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf>.

²⁸ Will Hurd, *Washington Needs to Adopt AI soon or We'll Lose Millions*, FORTUNE, (June 12, 2018), *online at* <http://fortune.com/2018/06/12/rep-will-hurd-artificial-intelligence/>.

²⁹ *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Mr. Gary Shapiro, CEO of the Consumer Technology Association).

³⁰ *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018)

from the McKinsey Global Institute reported that as a result of AI-driven automation, “up to 1/3 of [the] workforce in the United States and Germany may need to find work in new occupations.”³¹

Another study released by Oxford University in 2013 found the impact on U.S. workers by AI technologies may even be higher. According to the Oxford study, “about 47 percent of total U.S. employment is at risk.”³² These studies indicate the negative impact AI may have on jobs, which has the potential to increase wealth inequality in the United States.

Some of the hearing witnesses and other studies, however, show AI has the capacity to improve and increase jobs.³³ For example, the Organisation for Economic Co-operation and Development (OECD) released a study in March 2018 finding that about fourteen percent of jobs in OECD countries have a high risk of automation.³⁴ Additionally, a Deloitte study of 140 years of census data in the United Kingdom examined the effect of new technologies on jobs, and found in spite of new technologies, more jobs were ultimately created than eliminated.³⁵

The common thread from all of these studies is that our economic policies must take into account the uncertain future of work faced by Americans as AI takes hold, and the need for increased investments in education and worker retraining. As such, federal, state, and local agencies should be encouraged to engage more with educators, employers, employees, unions, and other stakeholders on the development of effective strategies for improving the education, training, and reskilling of American workers to be more competitive in an AI-driven economy. The federal government should also lead by example by investing more in education and training programs that would allow for its current and future workforce to gain the necessary AI skills.

Privacy

(statement of Ben Buchanan, Postdoctoral Fellow, Belfer Center Cyber Security Project, Science, Technology, and Public Policy Program, Harvard University).

³¹ McKinsey Global Institute, *Jobs Lost, Jobs Gained: Workforce Transitions In a Time of Automation* (Dec. 2017), *online at*

www.mckinsey.com/~media/McKinsey/Global%20Themes/Future%20of%20Organizations/What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/MGI-Jobs-Lost-Jobs-Gained-Report-December-6-2017.ashx.

³² CARL BENEDIKT FREY & MICHAEL A. OSBORNE, *The Future of Employment: How Susceptible are Jobs to Computerization?*, Comment, Uni. Oxford, (Sept. 17, 2013), *online at*

www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf.

³³ *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Mr. Gary Shapiro, CEO of the Consumer Technology Association).

³⁴ Organisation for Economic Co-operation and Development, *Putting faces to the jobs at risk of automation*, POLICY BRIEF ON THE FUTURE OF WORK, (March 2018), *online at* <https://www.oecd.org/employment/Automation-policy-brief-2018.pdf>.

³⁵ IAN STEWART, DEBAPRATIM DE, & ALEX COLE. *Technology and People: The Great Job-Creating Machine*, Deloitte (August 2015), *online at* <https://www2.deloitte.com/uk/en/pages/finance/articles/technology-and-people.html> (last accessed September 14, 2018).

AI technologies rely on computer algorithms that use data to determine how they will respond to new inputs.³⁶ Since AI requires vast amounts of data, witnesses in the Subcommittee’s hearings frequently cited individuals’ privacy as a potential challenge. For example, Dr. Ben Buchanan, an AI expert, testified about the various privacy risks consumers face when their personal data is used in AI systems.³⁷ According to Dr. Buchanan, “[t]here is the risk of breaches by hackers, of misuse by those who collect it or access it, and of secondary use—in which data collected for one purpose is later re-appropriated for another.”³⁸

These fears were realized when one of the nation’s largest credit reporting agencies, Equifax, Inc., announced in 2017 that hackers had successfully penetrated its systems, and gained access to the personal data of approximately 145.5 million Americans.³⁹ The data compromised included sensitive information Equifax had collected on consumers ranging from “Social Security numbers, birth dates, addresses, and in some instances, driver’s license numbers.”⁴⁰

Other examples where privacy concerns are implicated is the use of smart speakers that often feature voice-activated digital assistants. For instance, if a smart speaker is always listening in order to respond to a command, what is done with the hours of data it overhears? Law enforcement has already begun requesting voice recordings from technology companies for criminal cases. This raises the question of how devices that are always listening could potentially be used as evidence against consumers.⁴¹

To address the different privacy challenges raised by AI-driven technologies, one witness, Dr. Buchanan, testified before the Subcommittee that companies need to adopt more stringent safeguards in the design and development of their AI systems.⁴² However, other

³⁶ Tom Simonite, *The Wired Guide to Artificial Intelligence*, WIRED (Feb. 1, 2018), online at www.wired.com/story/guide-artificial-intelligence/.

³⁷ *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Ben Buchanan, Postdoctoral Fellow, Belfer Center Cyber Security Project, Science, Technology, and Public Policy Program, Harvard University).

³⁸ *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Ben Buchanan, Postdoctoral Fellow, Belfer Center Cyber Security Project, Science, Technology, and Public Policy Program, Harvard University).

³⁹ Equifax, *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident: Potentially Impacted U.S. Consumers Increased by 2.5 Million* (Oct. 2, 2017), online at <https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821>; Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), online at <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>.

⁴⁰ Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), online at <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>.

⁴¹ Jeff John Roberts, *Police Ask Amazon’s Echo to Help Solve a Murder*, FORTUNE (Dec. 27, 2016), online at <http://fortune.com/2016/12/27/amazon-echo-murder/>.

⁴² *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Ben Buchanan, Postdoctoral Fellow, Belfer Center Cyber Security Project, Science, Technology, and Public Policy Program, Harvard University).

witnesses, such as Dr. Oren Etzioni, CEO of the Allen Institute for Artificial Intelligence⁴³ and Gary Shapiro, President of the Consumer Technology Association,⁴⁴ argued that rather than trying to regulate all AI-related privacy issues under one umbrella, regulations should be tailored to individual AI applications. Some AI products and applications may already be subject to federal privacy laws, such as the *Health Insurance Portability and Accountability Act*, *Children’s Online Privacy Protection Act*, *Gramm-Leach-Bliley Act*, or fall under the jurisdiction of the Federal Trade Commission, the primary federal privacy regulator.⁴⁵

The growing collection and use of personal data in AI systems and applications raises legitimate concerns about privacy. As such, federal agencies should review federal privacy laws, regulations, and judicial decisions to determine how they may already apply to AI products within their jurisdiction, and—where necessary—update existing regulations to account for the addition of AI.

Biases

The increasing reliance on AI to make consequential decisions about individuals has also heightened concerns about the technology’s accuracy, particularly when used by governments. As the Electronic Privacy Information Center (EPIC) explained in a statement to the Subcommittee: “[w]hen the government uses AI to make decisions about people, it raises fundamental questions about accountability, due process, and fairness.”⁴⁶

At its core, AI is reliant upon data. If the data itself is incomplete, biased, or skewed in some other fashion, the AI system is at risk of being inaccurate.⁴⁷ As AI systems rely upon larger and larger quantities of data, the risk increases that the data sets may knowingly or unknowingly

⁴³ *Game Changers: Artificial Intelligence Part I: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Oren Etzioni, CEO, Allen Institute for Artificial Intelligence)

⁴⁴ *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Mr. Gary Shapiro, CEO of the Consumer Technology Association).

⁴⁵ See Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, (1996) (codified at 42 U.S.C. § 300gg and 29 U.S.C. § 1181 *et seq.* and 42 U.S.C. 1320d *et seq.*); Children’s Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728, (2000) (codified at 15 U.S.C. §§ 6501–6506); Federal Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), Pub. L. No. 106-102, 113 Stat. 1338, (1999) (codified at 15 U.S.C. §§6801-6809; §§ 6821-6827 and at 12 U.S.C. §1831u *et seq.*).

⁴⁶ Letter from Electronic Privacy Information Center to Rep. William Hurd, Chairman, Subcommittee on Information Technology, House Oversight and Government Reform Committee, and Rep. Robin Kelly, Ranking Member, Subcommittee on Information Technology, House Oversight and Government Reform Committee (April 19, 2018) (*online at* <https://www.epic.org/testimony/congress/EPIC-HCOGR-AI-Apr2018.pdf>).

⁴⁷ Tom Simonite, *The Wired Guide to Artificial Intelligence*, *Wired* (Feb. 1, 2018), *online at* www.wired.com/story/guide-artificial-intelligence/; National Science and Technology Council, *Preparing for the Future of Artificial Intelligence* (Oct. 2016) (*online at* obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf).

contain biases. There are legitimate concerns that if an AI system is trained on biased data, the AI system will produce biased results.⁴⁸

For example, in 2016, ProPublica began to investigate the use of computerized “risk prediction” tools by some judges in criminal sentencing and bail hearings. The investigation found the algorithm the systems relied upon was racially biased and inaccurate.⁴⁹ In total, African-Americans were “almost twice as likely as whites to be labeled a higher risk,” despite the fact those African-Americans who had been labeled high risk were subsequently found to not go on to commit another crime.⁵⁰ As AI technology is increasingly deployed into industries such as finance, law, and medicine, these biases could be reinforced by the technology, and harm populations.

During the Subcommittee’s hearings, witnesses and other stakeholders also made clear one of the most effective ways in which bias or potential biases in AI systems can be addressed is by increasing transparency in the use of these systems. As Dr. Charles Isbell explained in his testimony:

An AI system should [be] inspectable. The kind of data the algorithm uses to build its model should be available. The decisions that such algorithms make should be inspectable. In other words, as we deploy these algorithms, each algorithm should be able to explain its output.⁵¹

The solutions to addressing bias in AI are also cross-cutting. For example, Accenture recently introduced an “AI fairness tool,” which uses AI to examine how data influences variables, such as age, gender, and race in a model.⁵² Civil society groups, such as the Partnership on AI and the AI Now Institute, are also researching and engaging in discussions around bias and AI.⁵³

In short, addressing biases and potential biases in AI systems will necessitate improvements in transparency when those systems are used to make consequential decisions about individuals.

Federal, state, and local agencies that use AI-type systems to make consequential decisions about people should ensure the algorithms supporting these systems are accountable

⁴⁸ *Forget Killer Robots – Bias is the Real AI Danger*, MIT TECHNOLOGY REVIEW (Oct. 3, 2017), *online at* <https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/>.

⁴⁹ Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), *online at* www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

⁵⁰ *Id.*

⁵¹ *Game Changers: Artificial Intelligence Part 1: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Dr. Charles Isbell, Senior Associate Dean, College of Computing, Georgia Institute of Technology).

⁵² Natasha Lomas, *Accenture Wants to Beat Unfair AI with a Professional Toolkit*, TECHCRUNCH (June 9, 2018), *online at* <https://techcrunch.com/2018/06/09/accenture-wants-to-beat-unfair-ai-with-a-professional-toolkit/>.

⁵³ AI NOW INSTITUTE, <https://ainowinstitute.org> (accessed on Aug. 23, 2018); PARTNERSHIP ON AI, <https://partnershiponai.org> (accessed on Aug. 23, 2018).

and inspectable. In addition, federal, state, and local governments are encouraged to more actively engage with academic institutions, non-profit organizations, and the private sector in discussions on how to identify bias in the use of AI systems, how best to eliminate bias through technology, and how to account for bias.

Malicious Use of AI

The Subcommittee’s hearings also highlighted the need to prepare for and protect against the malicious use of AI. Earlier this year, OpenAI, a non-profit AI research company that testified at one of the hearings, co-authored a report finding that unless adequate defenses are developed, AI progress will result in cyberattacks that are “more effective, more finely targeted, more difficult to attribute, and more likely to exploit vulnerabilities in AI systems.”⁵⁴ The report’s findings are consistent with those from a 2017 survey conducted by the cybersecurity firm Cylance. According to the Cylance survey, “62 percent of [information security] experts believe artificial intelligence will be used for cyberattacks in the coming year.”⁵⁵

AI’s computing power enables it to increase the severity of cyberattacks exponentially. Three areas of malicious AI merit particular attention: political security; physical security; and digital security.⁵⁶ The common theme between these three spheres is AI expands the level of risk. For example, cyberattacks can affect more devices, people, and companies in a single moment, undermining digital security. In fact, the United States has begun to see cyberattacks against it using AI.⁵⁷

Consider the Russian disinformation campaigns of the past few years. With AI, “fake news” can be exponentially more convincing, with the potential to create videos of people making statements that they never made—known as “deepfakes”—as featured on Radiolab’s *Breaking News* episode last summer.⁵⁸ AI, using data, can pinpoint those who are most susceptible to disinformation with little human effort. This capability has the potential to greatly expand the number of people impacted in any disinformation campaign employed by hostile nation-states to disrupt another state’s political system.

Physical security can also be compromised by AI systems. For example, a team of researchers from American universities showed how autonomous vehicles could be tricked by hackers into misinterpreting stop signs with a few simple stickers that would otherwise appear innocuous.⁵⁹

⁵⁴ Miles Brundage, et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, (2018), online at https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf

⁵⁵ Cylance, *Black Hat Attendees See AI as Double-Edged Sword*, THREATMATRIX (Aug. 1, 2017), online at http://threatmatrix.cylance.com/en_us/home/black-hat-attendees-see-ai-as-double-edged-sword.html.

⁵⁶ Miles Brundage, et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, (2018), available at https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf.

⁵⁷ *The Morning Download: First AI-Powered Cyberattacks are Detected*, WALL STREET JOURNAL (Nov. 16, 2017), online at <https://blogs.wsj.com/cio/2017/11/16/the-morning-download-first-ai-powered-cyberattacks-are-detected/>.

⁵⁸ *RadioLab: Breaking News*, WNYC STUDIOS (July 27, 2017), online at <https://www.wnycstudios.org/story/breaking-news/>.

⁵⁹ David Z. Morris, *Researchers Show How Simple Stickers Could Trick Self-Driving Cars*, FORTUNE (Sep. 2, 2017), online at <http://fortune.com/2017/09/02/researchers-show-how-simple-stickers-could-trick-self-driving-cars/>.

As we consider all the positive ways AI will be used in the future, the government must also consider the ways it could be used to harm individuals and society and prepare for how to mitigate these harms.

How should the government respond to AI?

The U.S. government has traditionally taken a hands-off approach to emerging technologies. During the 1990s, the government's preferred policy when it came to the internet was to favor private action over public regulation. During that period, although Congress and state legislatures passed several laws governing commerce, content, and competition, they generally focused on crafting legal superstructures for the emerging web, not micromanaging its development; examples include the *Internet Tax Freedom Act*⁶⁰ and the *Telecommunications Act of 1996*.⁶¹ Concurrently, the Clinton Administration adopted a policy of salutary neglect. President Clinton ordered his administration to “do nothing that undermines the capacity of emerging technologies to lift the lives of ordinary Americans.”⁶²

It is the Subcommittee's recommendation that the federal government should approach any potential regulation of AI with the above history in mind. The government should begin by first assessing whether the risks to public safety or consumers already fall within existing regulatory frameworks and, if so, consideration should be made as to whether those existing frameworks can adequately address the risks. If those risks fall outside the existing regulatory framework, an approach should consider carefully whether modifications or additions are needed to better account for the addition of AI.

At minimum, a widely agreed upon standard for measuring the safety and security of AI products and applications should precede any new regulations. A common taxonomy also would help facilitate clarity and enable accurate accounting of skills and uses of AI. The National Institute of Standards and Technology (NIST) is situated to be a key player in developing standards. Similar private sector efforts exist from the Institute of Electrical and Electronics Engineers' Global Initiative on Ethics of Autonomous and Intelligent Systems.⁶³ The AI Index, which is a part of Stanford's “One Hundred Year Study on AI,” collects data about AI in order to track and measure its progress, which will be critical in the standards development process to provide historical context.⁶⁴ The federal government should look to support public, academic, and private sector efforts in the development of standards for measuring the safety and security of AI products and applications.

⁶⁰ Internet Tax Freedom Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681–719 (amending 15 U.S.C. § 151) (1998).

⁶¹ Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, (codified as § 47 U.S.C. 151 et. seq. (1996)).

⁶² Bill Clinton, President, and Al Gore, Vice President, Remarks by the President at and the Vice President at Electronic Commerce Event, (Nov. 30, 1998) (*online at* <https://govinfo.library.unt.edu/npr/library/speeches/rmkselec.html>) (last accessed September 17, 2018).

⁶³ IEEE Standards Association, *The IEEE Global Initiative on Ethics and Autonomous and Intelligent Systems*, (*online at* https://standards.ieee.org/develop/indconn/ec/autonomous_systems.html) (accessed on July 17, 2018).

⁶⁴ Artificial Intelligence Index, *Our Mission*, (*online at* <http://aiindex.org/#mission>) (accessed on July 17, 2018).

There are also tangible ways for the federal government to facilitate greater AI innovation absent regulation. For one, the government holds thousands of different data sets that could be useful to researchers studying AI and to agencies in accomplishing their missions. Many of these data sets are a public good and should be accessible to the public.

As such, the Senate should work to pass the OPEN Government Data Act (OGDA), which the House passed unanimously last year.⁶⁵ OGDA would allow for all non-sensitive government data to be made freely available and accessible to the public.⁶⁶ During the Subcommittee's hearings, several witnesses testified AI's development would be enhanced by more open data policies.⁶⁷ Provided the Senate passes OGDA, the President should sign it into law and the Administration should implement it as quickly as possible.

The Subcommittee also sees great value in encouraging innovation through national competitions. There should be a Grand Challenge, similar to DARPA's Grand Challenges, using data to solve a problem. The benefit of DARPA's Grand Challenges is their ability to foster innovative, collaborative research among teams seeking to overcome seemingly unattainable goals. Take, for example, DARPA's Self-Driving Car Challenge, which offered \$1 million to the first team to autonomously navigate a desert course from California to Nevada. In the first year of the Challenge, no team completed the course. In fact, the farthest any vehicle went was 7.5 miles. Yet eighteen months later, 5 out of the 195 competing teams completed the 132-mile course, with the winner having crossed the finish line in a little under seven hours.⁶⁸ DARPA's Grand Challenges provide strong incentives for innovation, and, as seen with its Self-Driving Cars Challenge, can effectuate quick technological advancement. Such competitions have spurred creativity, research, and collaboration, leading to some of the most groundbreaking inventions in recent history.

Another recommendation universally supported by witnesses at the hearings was a need for more financial support for R&D. The Subcommittee is encouraged by the research already occurring at universities and not-for-profits, as well as commercial R&D. The aggregate work of these bodies is why the United States is a leader in AI.

However, to maintain American leadership there is a need for increased funding for R&D at agencies like the National Science Foundation, National Institutes of Health, Defense Advanced Research Project Agency, Intelligence Advanced Research Project Agency, National Institute of Standards and Technology, Department of Homeland Security, and National Aeronautics and Space Administration. As such, the Subcommittee recommends the federal

⁶⁵ Foundations for Evidence-Based Policymaking Act, H.R. 4174, §201-202, 115th Cong. (1st Sess. 2017).

⁶⁶ Open, Public, Electronic, and Necessary (OPEN) Government Data Act, H.R. 1770, S. 760, 115th Cong. (1st Sess. 2017).

⁶⁷ *Game Changers: Artificial Intelligence Part 1: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Ian Buck, Vice President and General Manager, Tesla Data Center Business, NVIDIA); *Game Changers: Artificial Intelligence Part 1: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018) (statement of Amir Khosrowshahi, Vice President and Chief Technology Officer, Artificial Intelligence Group, Intel Corp.).

⁶⁸ Defense Advanced Research Projects Agency, *The DARPA Grand Challenge: Ten Years Later* (March 13, 2014), online at <https://www.darpa.mil/news-events/2014-03-13> (last accessed on September 17, 2018).

government provide for a steady increase in federal R&D spending. An additional benefit of increased funding is being able to support more graduate students, which could serve to expand the future workforce in AI.

CONCLUSION

AI has implications for every sector of industry and each Congressional committee should examine the role AI will play within their jurisdictions. To date, there have been six hearings held on AI: three by this Subcommittee; two by the Senate Committee on Commerce, Science and Transportation in 2016 and 2017; and one by the House Science, Space and Technology Committee in June 2018.⁶⁹ More oversight action by Congress is needed.

There is also a pressing need for conscious, direct, and spirited leadership from the Trump Administration. The 2016 reports put out by the Obama Administration's National Science and Technology Council and the recent actions of the Trump Administration are steps in the right direction. However, given the actions taken by other countries—especially China—Congress and the Administration will need to increase the time, attention, and level of resources the federal government devotes to AI research and development, as well as push for agencies to further build their capacities for adapting to advanced technologies.

The government has an essential role to play in securing American leadership in AI. Fulfilling this role will require balancing the creative energy of innovative Americans whose knowledge and entrepreneurial spirit have driven the development of this technology with regulatory frameworks that protect consumers. To ensure the appropriate balance is met, it is vital Congress and the Executive Branch continue to educate themselves about AI, increase the expenditures of R&D funds, help set the agenda for public debate, and, where appropriate, define the role of AI in the future of this nation. As our hearings have shown, these steps are necessary for the United States to remain at the forefront of AI advancement.

⁶⁹ *Game Changers: Artificial Intelligence Part 1: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018); *Game Changers: Artificial Intelligence Part II, Artificial Intelligence and the Federal Government: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018); *Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy: Hearing Before the Subcomm. on Information Technology of the H. Comm. on Oversight and Government Reform*, 115th Cong. (2018); *The Dawn of Artificial Intelligence: Hearing Before the Subcomm. on Space, Science, and Competitiveness of the S. Comm. on Commerce, Science, & Transportation*, 114th Cong. (2016); *Digital Decision-Making: The Building Blocks of Machine Learning and Artificial Intelligence: Hearing Before the Subcomm. on Communications, Technology, Innovation, and the Internet of the S. Comm. on Commerce, Science, & Transportation*, 114th Cong (2017); *Artificial Intelligence – With Great Power Comes Great Responsibility: Hearing Before the Subcomm. on Research and Technology and Subcomm. on Energy the H. Comm. on Science, Space and Technology Committee*, 115th Cong. (2018).