BROOKINGS

Report

Using AI and machine learning to reduce government fraud

Darrell M. West Friday, September 10, 2021

Editor's Note:

This report from The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET) Initiative is part of "AI Governance," a series that identifies key governance and norm issues related to AI and proposes policy remedies to address the complex challenges associated with emerging technologies.

Executive Summary

Artificial intelligence is being deployed in many different areas. Within higher education, it is used for college admissions and financial aid decisions. Health researchers employ it to scan the scientific literature for chemical compounds that may generate new medical treatments. E-commerce sites deploy algorithms to make product recommendations for consumers based on their areas of interest.[1]

But one of the most important growth areas lies in finance and operations. Both public and private sector organizations have large budgets to manage and it is important to operate efficiently and effectively. Accusations of budget inefficiencies or wasteful spending decrease public confidence and make it important to figure out how to manage resources in fair ways.

To help with budgetary oversight, AI is being used for financial management and fraud detection. Advanced algorithms can spot abnormalities and outliers that can be referred to human investigators to determine if fraud actually has taken place. It is a way to use technology to improve budget audits, personnel performance, and organizational activities.

Yet is it crucial to overcome several problems that plague public sector innovation: procurement obstacles, insufficiently trained workers, data limitations, a lack of technical standards, cultural barriers to organizational change, and making sure anti-fraud applications adhere to responsible AI principles.

In this paper, I make 10 recommendations for ways to overcome these issues so that managers and workers can gain the benefits of digital innovation without incurring serious ethical or operational problems. Among my specific recommendations are:

- Be proactive about developing responsible AI by hiring ethicists, creating review boards, and developing mitigation strategies early in product design and deployment.
- Use evidence-based evaluation to determine the efficacy of new projects.
- Expand the geographical opportunities for the technical workforce pool by encouraging remote or hybrid work.
- Develop partnerships with higher education, community colleges, technical institutes, online course providers, or firms offering personalized learning or certificate programs to train current and future workers.
- Embrace lifelong learning and expand professional development programs for technical and non-technical staff.
- Develop clear standards for data collection and analysis that will improve AI algorithms.
- Reform government procurement processes.
- Build a culture of innovation within the organization.
- Employ pilot projects to launch innovation in a less-risky manner.
- Figure out safe ways to scale up pilot projects to the entire organization.

The Federal Budget and COVID-19 Relief Funding

Operational efficiency is a particularly important issue in the federal government due to the sheer size of its overall budget. For fiscal year 2022, the national government is due to spend over $6 trillion, which is around 25.6% of the country's gross domestic product.[2] Of this amount, around $754 billion is devoted to national defense, $913 billion is for discretionary non-defense programs, and $3.7 trillion is for mandatory programs such as Social Security, Medicare, Medicaid, and others (with the remainder being interest on the national debt and other programs).[3]

In the wake of COVID-19, there have been large expenditures for pandemic relief over the past year. For example, in its Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020, Congress approved about $2.2 trillion, and the federal government allocated around $1.9 trillion in relief and economic stimulus through the American Rescue Plan Act of 2021. Much of this money was devoted to direct payments to those in need, help for businesses and nonprofits, aid to state and local government, and tax and spending changes.[4]

The large magnitude of the federal budget plus the enormous amount of money that has gone into American COVID-19 relief funding creates a need for tech-based monitoring to ensure that the money is going to intended recipients. With several trillion dollars allocated to a wide variety of organizations, it simply is impossible to employ traditional tools to track the money flows and adherence to agency guidelines. Antiquated computer systems are inadequate for the storage and analysis of large datasets, and the legacy software systems that remain prevalent in government computers are not up to the task of modern-day analytics.

In the early 2000s, Gregory Katz of the Government Accountability Office (GAO) testified before the House Committee on Homeland Security and made a number of important points about the challenges of relief programs. He noted several critical features of effective internal controls:

> **"*Upfront preventive controls* are the most effective and efficient means for reducing government fraud. Here, data mining, machine learning, and AI are powerful tools for strengthening government's ability to deter or prevent fraudulent activity *before* funds are disbursed.**
>
> ***Detection and Monitoring* serve as another vital threshold after payments have been initiated to ensure that claimants receiving funds are actually in need. Data mining, machine learning, and AI are also valuable for flagging abnormal patterns that can lead to the identification of fraudsters and the recovery of inappropriate payments.**
>
> ***Investigations and prosecutions* are costly, requiring large investments in human resources. Therefore, government agencies should focus on developing robust preventive controls as well as strong mechanisms for detection and monitoring."**[5]

In addition, a recent GAO report outlines several oversight risks in terms of COVID-19 relief. For example, the Paycheck Protection Program administered $670 billion through the Small Business Administration (SBA), yet the agency lowered its usual controls in order to get the money out the door rapidly. The Department of Labor, meanwhile, awarded $375 billion to states for unemployment insurance, but had to cope with a dramatic increase from 5.1 million claims in 2019 to over 42 million in 2020.[6]

At the very time when the need for fraud detection increased due to the rise in the amount of dollars and number of beneficiaries, assessing and tracking claims was very difficult because nearly every state had IT systems designed decades ago that did not facilitate data analysis or the monitoring of abnormal transactions. They did not share the same technical standards, and it was nearly impossible to see who returned to work but still received unemployment checks or whether they were eligible for full unemployment benefits.[7]

People can see that clearly in the case of the U.S. Treasury's Economic Impact Payments, which included stimulus checks totaling $282 billion. In that program, it was hard to oversee beneficiaries as the Internal Revenue Service (IRS) and Treasury Department "faced difficulties delivering payments to some individuals, and faced additional risks related to making improper payments to ineligible individuals, such as decedents, and fraud." As an illustration, the Treasury Inspector General for Tax Administration estimated that "1.1 million payments amounting to $1.4 billion had gone to decedents by April 30, 2020."[8]

There also were serious complaints about the SBA's relief program. Designed to aid struggling firms, the "SBA's much-vaunted new computer system ... proved blind to certain types of fraud and sometimes awarded grants even when it spotted disqualifying features." According to reports, "The amount stolen from the program, if it's ever tallied, will almost certainly be measured in the billions of dollars. But that's only part of the cost. Many legitimate applicants were denied grants because scammers got the money first."[9]

Traditional Fraud Detection

Given the magnitude of federal spending both in the domestic and defense areas, and especially with the amount of funding devoted to COVID-19 relief, it is important to take fraud detection and waste management seriously. Small percentages of spending that are wasteful, fraudulent, or abusive add up to large amounts of taxpayer dollars.

“Small percentages of spending that are wasteful, fraudulent, or abusive add up to large amounts of taxpayer dollars.”

In the days before advanced digital technologies, governments deployed a number of approaches to weed out fraud, waste, and abuse. For example, there were consumer hotlines where people could report misuse of federal money. Whistle-blowers could offer names, locations, and clarifying details regarding how funds were being misspent. Agencies then could launch investigations and determine whether the activities actually were fraudulent.

In addition, agencies could launch spot inspections where they showed up at a business, examined the operations, and reviewed financial records. Government inspectors could see for themselves if there were particular problems and collect evidence of possible wrongdoing. They could talk to executives and frontline workers and see if there were any suspicious activities that warranted additional investigation.

Finally, some offices uncovered fraud through internal audits, inspector general reports, or management reviews.[10] Agencies such as the IRS, Social Security Administration, the Centers for Medicare and Medicaid Services, the Veterans Administration, the Defense Department, the Department of Housing and Urban Development, the Federal Bureau of Investigation, and the Department of Health and Human Services have financial auditors who comb through budget information and government filings to see if there is wasteful spending.

According to a 2010 Association of Certified Fraud Examiners report, 46% of government fraud was identified through whistleblowers or hotline tips, 15% due to internal audits, and 12% based on management reviews. Less than 1% came from software or tech-based oversight, showing the relative paucity of digital oversight.[11]

Traditional methods are labor intensive, inefficient, and often ineffective. It is hard to gain detailed information through these approaches, and it requires lots of personnel and follow-up analysis—especially with multi-billion-dollar federal programs. Hotlines depend on people offering tips, and investigators have to sift through mounds of materials to find the cases warranting in-depth analysis. And once they identify those examples of possible fraud, they need trained investigators who can take advantage of the insights and turn the information into legal evidence.

AI for Fraud Detection

In an era of digital technology, there are new and powerful tools for investigating fraud. The wealth of data offered through electronic records, contracts, emails, text messages, and bank transfers allow officials to develop more advanced approaches to fraud detection. AI and machine learning are very well-suited for fraud detection because of the amount of digital information and ease of analyzing both text and data.

"In an era of digital technology, there are new and powerful tools for investigating fraud."

The key is getting AI into operational settings and mission priorities where it can help administrators do a more effective job. AI needs to be normalized as part of agency operations and not be a technical gadget that is separated from crucial missions within the organization. Integrating it into the agency mainstream helps employees understand the techniques and figure out how to deploy them in their particular arenas.[12]

The private sector already is deploying algorithms for fraud detection on a widespread scale and finding them to be valuable analytic tools. Banks, hospitals, educational institutions, and manufacturing firms use software to monitor financial transactions and make sure that both staffers and clients are following proper procedures.

To gain the benefits of technology, it is important for federal agencies to develop similar tools for financial oversight. AI represents a powerful way to analyze financial transactions, gain operational efficiency, and become more effective at investigating wasteful or unwarranted spending on a large scale. These techniques enable the public sector to improve its performance and do a better job safeguarding public resources.

The good news is there already are a number of federal agencies using AI. A 2020 report by researchers at Stanford and New York University for the Administrative Conference of the United States found that 45% of the 142 agencies surveyed were using AI and/or machine learning.[13]

According to that report and other research, there are a number of specific agencies developing AI tools for fraud detection and financial management. This includes the following examples:

- **Securities and Exchanges Commission**: Its Corporate Issuer Risk Assessment (CIRA) detects potential accounting and financial fraud, while the Advanced Relational Trading Enforcement Metrics Investigation System (ARTEMIS) and Abnormal Trading and Link Analysis System (ATLAS) rely upon algorithms that detect possible insider-trading. The Form ADV Fraud Predictor analyzes business submissions in order to determine whether companies represent high-, medium-, or low-risk categories.[14]
- **Internal Revenue Service**: The IRS has a modernization plan for "procuring software that completes laborious tasks in seconds through automation and artificial intelligence, eliminating error-prone manual work and increasing speed and accuracy."[15] The IRS also spent $400 million to design the Return Review Program (RRP), which compiles a fraud risk assessment for returns seeking refunds. It uses these tools to identify possible fraud and refer cases to investigators for in-depth analysis.
- **Centers for Medicare and Medicaid Services**: The agency has a Fraud Prevention Service (FPS) algorithm that analyzes claims data to assess fraud before and/or after payments are made. It also identifies providers with suspicious billing submissions in order to generate investigatory tips. The agency estimates that its systems have

helped to "prevent or identify nearly $1.5 billion in improper and potentially fraudulent payments from its implementation [in 2011] through the end of the calendar year 2015." The software has generated many leads and its officials claim that "25 percent of estimated savings from prepayment reviews were associated with FPS."[16]

- **Department of the Treasury**: For years, the department's Financial Crimes Enforcement Network AI System (FAIS) has examined suspicious money-laundering activities. The program has generated a number of investigations and recouped money from a large amount of fraudulent activities.[17] It takes advantage of the wealth of financial data to find abnormalities and suspicious behavior. Those cases then can be referred to human investigators to determine the legality of those actions.

These are just some of the ways federal agencies are incorporating AI in their operations. There are many illustrations across the national government of where AI is helping employees improve productivity, monitor financial transactions for illicit activities, and spot possible fraud. With additional training and better monitoring tools, government personnel could increase the scope and scale of the oversight.

Examples from Abroad

There are illustrations of other countries deploying AI and machine learning to reduce government fraud. This includes places such as the United Kingdom, where the Department of Work and Pensions has developed algorithms for processing social benefit claims. It deploys technology "to judge the likelihood that citizens' claims about their childcare and housing costs are true when they apply for benefits." The AI brings together information from a variety of sources such as law enforcement, benefits offices, the land registry, and personal credit to assess whether people warrant social benefits.[18]

The Organization of Economic Cooperation and Development is focused on ways to implement broad AI principles. Using a multi-stakeholder taskforce, it is encouraging AI investment in the public sector, focusing on workforce development, building data infrastructures that will facilitate AI deployment, and developing key ethical principles that will guide responsible agency operations.[19]

In some countries, though, AI has become a subject of controversy. The Netherlands implemented a System Risk Indication algorithm to assess fraud in government programs. It examined people's claims and their financial backgrounds to see if they legitimately warranted the benefit. Yet the program was deemed illegal by a district court for failing to "strike a fair balance between the interference with the right to respect for private life and the benefits of the use of new technologies to prevent and combat fraud."[20]

This and other examples represent demonstrate the need for the implementation of responsible AI that respects basic rights. An analysis by the World Economic Forum found that "65% of government entities surveyed planned to adopt AI tools and 85% planned to implement big data analytics by 2025."[21] The reason is simple. As noted in a McKinsey report, executives believe such investments will pay off in increased savings. Its authors write, "We've seen returns on investment ranging from 10:1 to 15:1. These stories provide a road map for successfully improving detection and prevention that is applicable across a wide range of institutions."[22]

Barriers to AI Usage

Although AI tools exist for fraud detection and financial oversight, it is not always easy to implement them operationally, introduce new digital tools, or integrate them into agency missions. There are a number of barriers to AI and machine learning innovation in the federal government. For example, the procurement process is complicated and difficult for many companies to navigate. Even large firms that have lots of experience with federal paperwork and processes find it challenging to expedite the process. Current rules require a lengthy and detailed sequence of activities that include scoping out the job, an analysis of task alternatives, requests for proposals, formal analysis of competing bids, and an appeals process if losing competitors object to the way things were handled, among other things.

Many national agencies lack a procurement workforce with the skills necessary to purchase and assess AI algorithms. They have problems in figuring out the best way to procure advanced technology products and services. One of the crucial decisions is whether to develop their own software that is personalized to their own particular needs, buy proprietary software off the shelf, or rely on third-party developers. But in any of those alternatives, agencies need people who understand algorithms in order to make prudent decisions that yield actionable and scalable information.

In a 2020 publication, the Administrative Conference of the United States reports that about half of government agencies' current AI applications were developed by in-house personnel customized to support their particular needs; the rest relied upon third-party or commercially available products.[23] However, a number of the in-house solutions were not fully implemented, and it is not clear whether they were able to achieve stated objectives.

Within many agencies, there are cultural and structural barriers to change. These include a reluctance to innovate, preference for the status quo, fear of failure, being overly siloed so that different divisions handle various data and parts of essential missions, and not having leaders and managers who are skilled at facilitating change. In many organizations, the barriers to change are not just about the technology, but about the structure, operations, management, and culture of the agencies. Unless leaders are committed to building an innovation culture, the adoption of new technologies almost always will fall short of their intended benefits.[24]

"Unless leaders are committed to building an innovation culture, the adoption of new technologies almost always will fall short of their intended benefits."

In addition, there are issues related to data and technical standards. One of the key features of any algorithm is its data. If the data come in non-standard or unstructured form, it becomes more difficult to make effective use of that information. It is hard to input the material, difficult to compare, and challenging to analyze the material. Non-standardized and non-integrated information can create more noise than signal, clouding the analysis of the relevant material and making it impossible for investigators to proceed with fraud cases.

Similar obstacles occur in regard to video images. There is software that can process and analyze pictures and images, but a number of the commonly used systems have inaccuracies and/or biases that limit their utility. The images need to be tagged with appropriate identifiers in order to maximize their utility. They don't always work well with protected categories of individuals or achieve the objectives that managers desire.

Data sharing remains a major challenge as well. Many agencies would benefit from integrating datasets in ways that would provide greater insight, yet it is hard to do this because of unstructured data, incompatible operating systems, and federal privacy rules that preclude information sharing across departments and divisions. There are so many restrictions on integrating data bases across functional areas that it limits the ability to take full advantage of digital technologies. This slows the adoption of artificial intelligence and machine learning tools in the federal government and delays the use of anti-fraud applications.

Concern over privacy, security, cybersecurity, and ransomware complicates the innovation ecosystem in public and private sector organizations. It is tricky to balance all the competing requirements of an effective IT system, which includes protecting personal privacy, making sure confidential information is not compromised, and guarding against outside entities taking control of computer systems.

In today's world, cybersecurity and ransomware vulnerabilities plague many information systems, and create problems for AI algorithms. It is hard to protect critical infrastructure, health-care systems, financial networks, government agencies, and commercial enterprises in an era of foreign intrusions and criminal enterprises.[25]

Workforce training

There needs to be broad-based and advanced technology training for the public workforce. It does not mean everyone has to become a coder or software designer, but a broader swath of federal employees has to know enough about algorithms, software applications, and IT systems in order to evaluate the algorithms, understand possible AI risks, and take steps to mitigate known problems. Employees must be digitally literate even if they do not have a technical position or direct oversight of algorithms.

One of the hardest workforce issues is finding the kind of talent needed for AI innovation. In addition to technical experts, federal agencies need lawyers, policy experts, social scientists, and ethicists who understand the negative ramifications of artificial intelligence. Due to biased decisions or a lack of transparency, there are many things that can go wrong with algorithms and lead to a negative impact on human safety, privacy intrusions, and workforce harms. Having workers who are skilled in these areas is vital for technology innovation.

Despite these crucial needs, it is hard for the public sector to outbid and out-hire commercial firms. There is a high level of competition for a limited supply of technical talent, and this makes it difficult for government agencies to obtain needed personnel.[26] The United States does not graduate a sufficient number of students with a strong understanding of AI, machine learning, and data analytics, and this makes it challenging to deploy these tools within federal agencies.

But there are several steps that could ease the challenges of workforce development. One is that in a COVID-19 world of remote or hybrid work, government agencies can draw on a wide range of technical talent across the country. Workers do not need to live in Washington, D.C., to work for a federal agency, and the growth of remote work expands the talent acquisition pool for the entire government. Geography no longer limits the hiring of tech talent in the public sector or gaining access to online training platforms.

A number of government agencies are developing partnerships with higher education that help them train current workers and acquire future talent. There are many entities that provide appropriate training such as four-year schools, community colleges, technical institutes, online course providers, or private firms that offer certificate programs. The blossoming of new training programs offers federal workers a chance to upgrade their job skills throughout their lifetimes.

"Government agencies need to move toward a model of lifelong learning where people acquire skills throughout their career, regardless of their age."

Government agencies need to move toward a model of lifelong learning where people acquire skills throughout their career, regardless of their age.[27] Organizations need to provide ongoing professional development opportunities as technology transforms the skills needed in their workforce. Offering tuition reimbursement programs, covering course costs, or paying for online instruction or certificate programs should be a high priority for public sector organizations. There is proposed legislation, including the AI Training Act, that would help workers gain new skills.

Finally, agencies furthermore can develop partnerships with private companies for cyber corps that provide short-term stints in government or project-oriented opportunities that allow those in the business world to provide their expertise in areas needed by the agency. For example, the Michigan Civilian Corps is a group of cybersecurity professionals that the governor can call upon to assist in a cyber emergency, augmenting the state's response capability. Arrangements like these would expand the talent pool and help government offices recruit new people on a short-term or contractual basis, and address key workforce needs.

Procurement reform

There needs to be reform of the federal procurement process to make it easier for qualified firms to supply needed products. It is difficult for companies that are inexperienced in selling products and services to the government to figure out where to go, what to do, what forms need to be provided, and what clearances and certifications have to be gained. Streamlining and expediting procurement processes is vital to improve the federal government's capacity for technology innovation.[28]

One useful development is the rise of AI templates that can be adapted to organizational needs. In the same way that some types of data analysis and statistical modeling have been standardized, templates make it easier for non-specialists to use AI and machine learning. As long as they are attuned to nuances and particular specifications, automated AI packages can help agencies deploy innovative solutions. Updating procurement processes to take advantage of templates and standardized programs would speed technology innovation in the federal government.

In addition, making sure that minority-owned firms and those led by women have fair opportunities to compete for federal contracts is vital for improving the equity of government procurement. Right now, some of those firms face disadvantages due to a lack of experience with procurement processes or structural barriers that limit their chances to compete. Ensuring equitable processes will put people on a level playing field and lead to fairer outcomes.

Technical standards

In order to fulfill the requirements of algorithms, we need clear standards for data collection and analysis. There has to be more uniform standards about how information is compiled, coded, analyzed, and interpreted to make AI useful, fair, and unbiased. Reaching common agreements or having technical standards on how datasets are organized would unleash opportunities for more powerful AI deployments in the public sector.

This is especially the case for application programming interfaces (APIs). There needs to be way to transmit and connect data systems so that information is available and can be used to improve real-time decision-making. One of AI's virtues is its capacity to learn as it goes along and improve the way it makes decisions. But having clear data and technical standards is necessary in order to reach these kinds of goals.

Appropriately handling operational decisions will be crucial as well, such as whether to keep the data on particular devices or move them to cloud storage sites, how to make data accessible to developers who need to the information, and how to build information pipelines that facilitate analysis and interpretation. An inability to address these crucial operational considerations will doom new digital innovations to failure.

The National Institute for Standards and Technology is undertaking constructive efforts in this regard, as is the Joint Artificial Intelligence Center in the defense area. Each entity has brought together experts from government, business, and academia to think about technical standards and ways to implement proper AI standards. Political leaders should encourage and support those efforts, as well as similar activities being undertaken by a number of technical standards organizations.

Creating a culture of innovation

Creating a culture of innovation is one of the most challenging steps that government officials can undertake in order to break through bureaucratic inertia and encourage responsible AI adoption. They need to instill in their structures, operations, and management styles the idea that change is helpful and experimentation is desirable. Pilot projects should be established for small-scale AI applications that do not hurt the general public, but provide agency experience in algorithm development and deployment. Projects that prove successful can be scaled up and deployed more broadly.

"Creating a culture of innovation is one of the most challenging steps that government officials can undertake in order to break through bureaucratic inertia and encourage responsible AI adoption."

It is difficult to know how to build these kinds of organizational cultures, but management leadership plays a key role. Government officials need to create "sandboxes" for experimentation that provides low-risk chances to design new products and services and test them in a limited way. This will help refine the products and reduce the problems when large-scale deployment takes place.[29] It inculcates a culture of change that, in the long run, will improve agency operations and lead to a workforce that is willing to experiment, take acceptable risks, and learn how to deploy digital products more effectively.

In her book "Solving Public Problems," New York University Professor Beth Simone Noveck argues that government leaders need to train people in new ways of thinking and working. She says it requires individuals engaging in crowdsourcing, collaboration, and building co-designed products. Compiling evidence and prioritizing experimentation are vital for forward-leaning public agencies, and she notes that we must get smart with "data and people."[30]

Scaling up innovation

It is crucial for agency leaders to figure out how safely to scale up innovation. Private companies often develop new products and test them on pilot samples before extending them more broadly throughout the community. That helps them evaluate the deployment and learn how people are using and being affected by the new applications. It is a way to safeguard the innovation process and provide guardrails for product rollouts.

The federal government needs to develop similar processes. It almost never is a good idea to launch new software on millions of people simultaneously; there always are going to be bugs, defects, and unanticipated outcomes that inflict possible harms. Having processes that start small, identify problems, and mitigate them before large-scale deployment helps agencies avoid embarrassing failures that make the government look inept.

Agencies need some means of learning from one another. Right now, each department is reinventing the wheel and wasting valuable time on moving up the learning curve. Federal executives should share their best practices and take advantage of the successes and failures that each entity experiences. There is no reason for people to make the same mistakes in different settings when better communications and coordination could avoid particular problems.

Using AI responsibly

One of the biggest AI challenges is figuring out how to convert broad ethical principles such as fairness, equity, privacy, transparency, accountability, and human safety to specific deployments. These types of principles sometimes conflict with one another, and leaders need to examine what fairness means and how to judge AI algorithms. Some agencies, such as the Equal Employment Opportunity Commission, employ an 80%-20% disparate impact rule that means it expects hiring decisions to fall within four-fifths of the rate across demographic categories.[31]

Guidelines such as that can offer software designers rules that already have been utilized within federal agencies to assess whether there is unfairness or outright bias in algorithmic decisions. Software that generates large disparities across protected groups should be flagged for additional analysis to determine why that is happening and how to reduce the disparities.

In addition, there are procedural reforms that would improve the use of AI for government anti-fraud investigations. To become more proactive about ethical considerations, government agencies should develop internal review boards similar to university human subjects committees that assess proposed innovations and seek to anticipate and mitigate possible problems. Rather than deploying untested products and rushing to deal with unanticipated problems or faulty designs, there can be processes staffed by appropriate ethicists and experts that can help specialists and generalists alike think about AI innovation. These experts can help agencies avoid problems and be more forward-looking in tech deployments.[32]

Finally, having evidence-based assessment built into the process is key for responsible AI. It is vital to compile evidence on the impact of AI across protected categories and how people are being affected by the algorithm. Effective evaluation needs to go hand-in-hand with good product design.[33] Having clear-cut data analysis and policy assessment will inform AI design and deployment, and lead to products that are safer, fairer, and more effective in achieving their objectives.

Conclusion

To summarize, it is an exciting time for responsible AI innovation in the federal government. Algorithms are transforming agency performance in many areas and helping to improve worker productivity, service delivery, and financial oversight. Yet there remain major challenges that must be overcome in order to gain the full benefits of the AI revolution. There are a number of reforms that, if adopted, will make AI more responsible, will train the workforce, and allow agencies and departments to be more effective in monitoring budgetary and financial transactions. Making progress in these areas will enhance public sector action and provide taxpayers with greater confidence regarding government performance.

Thanks to Hattie Pimentel and Emily Skahill for outstanding research assistance on this report.

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.

Microsoft provides support to The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET) Initiative. The findings, interpretations, and conclusions in this report are not influenced by any donation. Brookings recognizes that the value it provides is in its absolute commitment to quality, independence, and impact. Activities supported by its donors reflect this commitment.

Report Produced by **Center for Technology Innovation**

Footnotes

1. 1 Darrell M. West and John R. Allen, *Turning Point: Policymaking in the Era of Artificial Intelligence*, Brookings Institution Press, 2020.
2. 2 White House, *Budget of the U.S. Government*, Office of Management and Budget, p. 42.
3. 3 White House, *Budget of the U.S. Government*, Office of Management and Budget, p. 42.
4. 4 National Association of Counties, "American Rescue Plan Act Funding Breakdown," undated.
5. 5 Gregory Katz, "Individual Disaster Assistance Programs: Framework for Fraud Prevention, Detection, and Prosecution," Testimony Before U.S. Committee on Homeland Security, July 12, 2006.
6. 6 Government Accountability Office, "COVID-19: Opportunities to Improve Federal Response and Recovery Efforts," June 25, 2021.
7. 7 Government Accountability Office, "COVID-19: Opportunities to Improve Federal Response and Recovery Efforts," June 25, 2021.
8. 8 Government Accountability Office, "COVID-19: Opportunities to Improve Federal Response and Recovery Efforts," June 25, 2021.
9. 9 Michelle Davis, Zachary Mider, and Polly Mosendz, "An Avalanche of Fraud Buried a Small Business Relief Program," *Bloomberg Businessweek*, October 29, 2020 and William Shear, "Small Business Administration: COVID-19 Loans Lack Controls and Are Susceptible to Fraud," Testimony Before U.S. House Committee on Small Business," October 1, 2020.
10. 10 Charles Dempsey, "The Inspector General Concept," *Classics of Administrative Ethics*, Routledge, 2001.
11. 11 Association of Certified Fraud Examiners, "Report to the Nations on Occupational Fraud and Abuse," 2010.
12. 12 Thanks to Charles Audet and Ernest Sohn of Booz, Allen, Hamilton for sharing their observations with me on AI issues.
13. 13 David Freeman, Daniel Ho, Catherine Sharkey, and Mariano-Florentino Cuellar, "Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies," Administrative Conference of the United States, February, 2020.
14. 14 David Freeman, Daniel Ho, Catherine Sharkey, and Mariano-Florentino Cuellar, "Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies," Administrative Conference of the United States, February, 2020.
15. 15 U.S. Department of Treasury, "Treasury Announces IRA Integrated Modernization Business Plan Promoting Cost Efficiency, Improved Taxpayer Service and Protection," April 18, 2019.
16. 16 Government Accountability Office, "CMS Fraud Prevention System Uses Claims Analysis to Address Fraud," August, 2017.
17. 17 U.S. Department of the Treasury, "FinCEN's IT Modernization Efforts," July 12, 2021.
18. 18 Robert Booth, "Benefits System Automation Could Plunge Claimants Deeper Into Poverty," *The Guardian*, October 14, 2019.
19. 19 Organization of Economic Cooperation and Development, "State of Implementation of the OECD AI Principles: Insights From National AI Policies," June, 2021.
20. 20 Library of Congress, "Netherlands: Court Prohibits Government's Use of AI Software to Detect Welfare Fraud," March 13, 2020.
21. 21 World Economic Forum, "The Future of Jobs Report," October, 2020.
22. 22 Susan Cunningham, Mark McMillan, Sara O'Rourke, and Eric Schweikert, "Cracking Down on Government Fraud with Data Analytics," McKinsey, October 15, 2018.
23. 23 David Freeman, Daniel Ho, Catherine Sharkey, and Mariano-Florentino Cuellar, "Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies," Administrative Conference of the United States, February, 2020.
24. 24 Darrell M. West, *Digital Government, Technology and Public Sector Performance*, Princeton University Press, 2005.
25. 25 Rachel Lerman and Gerrit De Vynck, "Widespread Ransomware Attack is Affecting Hundreds of Businesses," *Washington Post*, July 2, 2021.
26. 26 Ryan Tracy, "How Can Government Attract the AI Talent It Needs"", *Wall Street Journal*, April 6, 2021.
27. 27 Darrell M. West, *The Future of Work: Robots, AI, and Automation*, Brookings Institution Press, 2018.

28. 28 Steven Koltai, “The Mouse and the Hippo: Solving Problems in Procurement,” *Devex*, October 10, 2016.
29. 29 David Freeman, Daniel Ho, Catherine Sharkey, and Mariano-Florentino Cuellar, “Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies,” Administrative Conference of the United States, February, 2020.
30. 30 Beth Simone Noveck, *Solving Public Problems: A Practical Guide to Fix Our Government and Change Our World*, Yale University Press, 2021.
31. 31 Society for Human Resource Management, “Avoiding Adverse Impact in Employment Practices,” June 18, 2020.
32. 32 Darrell M. West and John R. Allen, *Turning Point: Policymaking in the Era of Artificial Intelligence*, Brookings Institution Press, 2020.
33. 33 Commission on Evidence-Based Policymaking, “The Promise of Evidence-Based Policymaking,” September, 2017.