Government Inc.: Amazon, Government Security & Secrecy

A Report By

OPEN THE GOVERNMENT

About Open the Government (OTG)

Open the Government is an inclusive, nonpartisan coalition that works to strengthen our democracy and empower the public by advancing policies that create a more open, accountable, and responsive government.

The Authors

Emily Manna, Co-Author: Manna's policy work at OTG centers on transparency and accountability for U.S. military and national security programs and records management and data preservation. She holds a Master's in Public Policy from Georgetown University, where her research focused on the U.S. drone program and a B.A. from American University.

Jesse Franzblau, Co-Author: Franzblau carries out policy analysis, conducts monitoring and evaluation of federal information policy, and helps coordinate OTG's government relations program to advance the policy priorities of the coalition. He manages OTG's freedom of information projects, coordinating efforts to use transparency laws to increase access to information on government surveillance, policing, and immigration enforcement.

Connect with Open the Government

Openthegovernment.org

Acknowledgements

Open the Government expresses deepest appreciation to the following individuals and organizations whose valuable insight and expertise enriched and helped shape this report.

Journalists

Patrick Tucker, Defense One; Frank Konkel, Nextgov; Jenna McLaughlin, Yahoo News; Jason Leopold, Buzzfeed.

Individuals & Organizations

Scott Amey: Jake Laperruque, Project On Government Oversight*
James Thurber, American University
Paromita Shah, National Immigration Project of the National Lawyers Guild*
Amie Stepanovich, Access Now
Clare Garvie; Georgetown Law Center on Privacy & Technology
Deborah Raji, University of Toronto
Jeramie Scott, Electronic Privacy Information Center*
Trevor Timm, Freedom of the Press Foundation
Good Jobs First*
Electronic Frontier Foundation*
MuckRock*
Center for Responsive Politics*
Fight for the Future
Mijente
Immigration Defense Project

Editors & Graphic Design

Lisa Rosenberg, Executive Director, Open the Government
Ufuoma Otu, Communications Director, Open the Government

**OTG Partner Organization*

Table of Contents

Executive Summary

Amazon is preparing to locate its second headquarters just outside Washington D.C., but because so much of the government "runs on Amazon," the company already essentially occupies suites within dozens of state and federal agencies, including the Central Intelligence Agency, the Department of Homeland Security and local law enforcement agencies. The company does not provide mere office supplies or routine tech services. Instead, the government relies on Amazon to supply artificial intelligence (AI), machine learning, and biometrics data systems; technology that is opaque, hard to understand and has few safeguards.

Of course, many other corporations, including Microsoft, Google, IBM and a host of startups profit from government contracts to provide myriad government entities with advanced technology. Amazon, however, is poised to secure dominance of cloud-related government contracts in the years to come. Among other contracts, Amazon is the frontrunner for what may be the largest government IT contract in history-the Pentagon's $10 billion, 10-year Joint Enterprise Defense Infrastructure (JEDI) program.

Amazon is often less transparent than its competitors in terms of providing the public with information about its government contracts, compounding concerns about its provision of controversial technologies. Its facial recognition software, which studies show suffers from bias and inaccuracies, is used for surveillance by police, is being piloted by the FBI, and has been pitched to Immigration and Customs Enforcement. The Department of Homeland Security relies on Amazon's cloud services for its information sharing, border security and immigration enforcement operations. Its cloud computing services bestow AI and machine learning capabilities throughout the national security apparatus, and the Department of Defense hopes to use such technology to "support lethality and enhanced operational efficiency."

Whenever private companies enter the government space, they operate with much less public scrutiny than when government employees do the same work directly. Private companies do not have the same transparency requirements as government agencies, and the accountability mechanisms for contractor failures, waste, fraud, and abuse are therefore much weaker. In addition, the ubiquity of nondisclosure agreements between the government and its contractors severely limits access to information about the work being done.

Moreover, the technology itself is opaque. The more complex the algorithms involved in an AI system, the more difficult it is for anyone, including the system's human creators, to discern what went into the answer the computer spits out.

The combination of secretive corporate contractors and inscrutable technology increases the risk of harm ranging from privacy violations to discriminatory policing to military decisions made without human intervention. To mitigate the risk, the public must demand transparency from and ensure oversight of government contractors.

This report offers recommendations to federal, state and local governments, as well as to the private sector, to ensure rigorous transparency and accountability rules are in place when private actors perform government operations.

Recommendations for governments

Federal, state and local government entities must establish strict safeguards before purchasing and deploying AI technologies, including facial recognition systems and cloud computing services. To exercise oversight, they must mandate transparency from companies regarding the capabilities and limitations of the technology, including strengthening public records and mandatory reporting laws. Government entities must have the resources to hire staff that understands the technology, and address loopholes in lobbying disclosures to better discern the ways in which private companies influence the procurement process.

Governments have a duty to protect the public by establishing limits on collection, use, and retention of data by government technology contractors. They must investigate whether facial recognition and other technologies have a disparate impact on communities of color. They must provide the opportunity for public notice and comment prior to the procurement of facial recognition software.

Recommendations for companies

Companies must limit the sale of AI technologies unless mechanisms and strong safeguards are in place to prevent abuse, and they have a commitment from the agencies with which they contract to specify how technologies will be used. Companies must develop and publicly release AI principles and policy frameworks to improve transparency reporting, including improving how to explain AI systems to the public. They must refrain from implementing nondisclosure agreements or other legal barriers that stand in the way of accountability in the public sector.

Recommendations for members of the public

Journalists, academics and advocacy organizations must investigate the companies contracting with military, police, intelligence, and immigration agencies. They must look into the risks associated with the technologies and the potential impact on vulnerable communities. Advocates must defend the rights of employees who object to their work being used to enable human and civil rights abuses. The public must support legislative efforts to limit the influence of corporations on the federal procurement process, and demand effective oversight from lawmakers.

Introduction

Amazon is notorious for its secrecy, stonewalling even basic inquiries most Fortune 500 companies would consider routine.[i] The company routinely tries to prevent government bodies from responding to public records requests, and often refuses to be named in negotiations to open its data centers across the country, instead using the name of one of its subsidiaries, Vadata, Inc.[ii] Industry watchers were not surprised, therefore, that Amazon was tight-lipped about where it would build additional headquarters. For a year, cities across the country competed to host the company's expansion, offering subsidies, tax cuts, and other incentives to bring Amazon jobs to their regions. In true Amazon fashion, the details of the offers were sealed. Every city that made Amazon's top list for its HQ2 had to sign a nondisclosure agreement with the company.[iii] So, when Amazon announced in late 2018 that its highly-anticipated choices were New York City and a Northern Virginia suburb of Washington, D.C., many other U.S. cities felt they had been taken for a ride.

After all, the winners turned out to be two cities that not only already had booming economies, but where Amazon chief Jeff Bezos also happens to own homes. In the case of D.C., Bezos had purchased the region's largest newspaper, The Washington Post, five years prior. The D.C. region is also home to the east coast headquarters for Amazon Web Services, the company's flourishing subsidiary and the largest cloud services provider in the country. It seemed to many that the "competition" for HQ2 had really just been an elaborate scheme to get as many financial incentives as possible out of the winners.[iv]

In February, Amazon announced that it would not move forward with the planned New York expansion, in response to significant pushback from the public and from local, state, and federal legislators. In the wake of the NYC fallout, organizers and lawmakers are also ratcheting up opposition to the HQ2 development planning in Northern Virginia.[v]

Data center. iStock/Getty Images

Despite the opposition, progress on the Northern Virginia headquarters appears to be moving ahead as planned, deepening the ties-and the access-the company already has with the region. Amazon has contracts across the federal government, directly and indirectly through private sector partners who use AWS cloud services themselves. Amazon does not release specific numbers, but analysts predict the company's total U.S. government business for 2019 could rise to as much as $4.6 billion.[vi]

"The high concentration of tech companies, federal agencies, and supporting organizations offer Amazon the opportunity to develop valuable future relationships," according to Virginia's winning HQ2 proposal. "Northern Virginia provides an unmatched place for Amazon to locate as it attempts to influence federal policies, particularly as it delves into complex areas of federal regulatory authority (e.g., unmanned drones).”[vii]

Amazon is not alone. Private contractors make up about 40 percent of the federal government work force, according to research by New York University professor Paul Light.[viii] That means the private sector is performing an immense amount of work on behalf of and paid for by U.S. taxpayers, but with much less public scrutiny than if the work were being done by government employees directly. Private companies do not have the same transparency requirements as government agencies, and the accountability mechanisms for contractor failures, waste, fraud, and abuse are therefore much weaker. Government contractors assert their status as private entities to exempt themselves from the Freedom of Information Act, and even FOIA requests to the government about work done by contractors are subject to exemptions that severely limit access to information. Absent transparency requirements, a growing tide of tech workers are turning into whistleblowers to expose serious ethical abuse and human rights violations as they occur. Silicon Valley employees continue to call on Microsoft, Google, and other tech giants to stop contracting with the government on matters of war, immigration enforcement and policing.

> ***“Northern Virginia provides an unmatched place for Amazon to locate as it attempts to influence federal policies, particularly as it delves into complex areas of federal regulatory authority (e.g. unmanned drones)”***
> ***- Virginia’s winning HQ2 proposal***

When examining the potential-and danger-of private government contracting, it’s difficult to find a better case study than Amazon. Bezos is the world’s richest man, and Amazon paid $0 in corporate income taxes last year despite nearly $11 billion in profits thanks to tax loopholes and subsidies.[ix] AWS is now Amazon’s biggest money-maker, with government contracts making up about 10 percent of AWS’ profits. Amazon has drastically increased its lobbying expenditures over the past several years,[x] and appears poised to expand its dominance of cloud-related government contracts in the years to come.

Amazon also crystallizes and exacerbates the problems of clandestine government contracting. The company is ripe for scrutiny as a result of its long reach into the work of the federal government combined with its culture of corporate secrecy. Even more concerning is that much of the technology Amazon provides the federal government may be dangerous, and is poorly understood by the public, policymakers, and even its own creators.

Amazon’s facial recognition software, Rekognition, has grown increasingly controversial as research begins to accumulate showing the technology has inherent bias and accuracy problems, fueling invasive and discriminatory police surveillance. Amazon pitched Rekognition to Immigrations and Customs Enforcement (ICE) in 2018, and in 2019 the FBI announced it will be piloting the software. Amazon sells cloud and AI services that have become the tech backbone for the Department of Homeland Security's detention and deportation machine.

Agents arrest suspects. Photo Courtesy of ICE

Amazon's cloud computing services and artificial intelligence development for military and the intelligence community is even more opaque. The company has provided these technologies to the intelligence community since 2013 and is now the frontrunner for a similar but even larger contract-the so-called JEDI contract-with the Department of Defense (DoD), due to be awarded in 2019. The public has very little access to information about how the intelligence community is using these services, and how Amazon's AI systems may be incorporated into government counterterrorism and national security programs. DoD promises to integrate AI across the entire department, raising serious questions about the future of technology that still has few safeguards. The combination of private sector influence, national security secrecy, and dangerously powerful technology is a significant threat to government accountability.

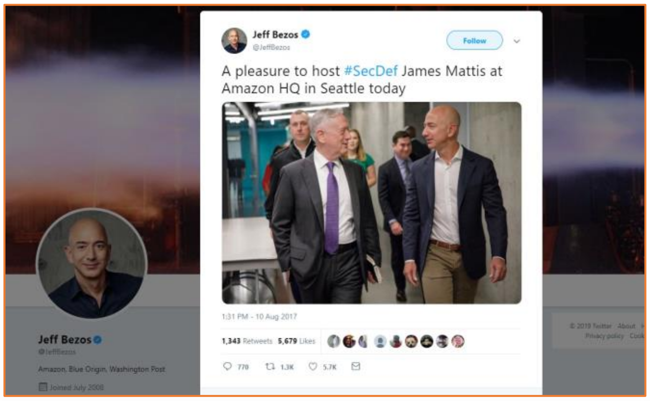
Amazon, which did not respond to multiple questions sent by OTG or to requests for comment, is a multi-headed Hydra of corporate purveyors of advanced technology to the government, due to its reach into the intelligence community, federal agencies, state and local law enforcement, and possibly soon the military. But it is hardly alone. All corporations seeking the bounty of government contracts in the fast-growing AI sector face questions as to how willing they are to provide technology for government missions they, or their employees, oppose, and how willing they are to be held accountable when their technology is used. More critically, by relying on secretive corporate contractors to provide AI and machine learning, our government puts all of us at risk of harms ranging from privacy violations to misidentification to military decisions informed by black box algorithms. Every level of government must work to ensure laws keep up with technological advances, and demand transparency from and engage in oversight of government contractors. Any arm of government that uses advanced technology must also ensure it has the resources, in terms of human intelligence, to dissect and understand the technology it is employing.

Part 1: The government runs on Amazon

Amazon's most expansive foray into government has been through its Amazon Web Services (AWS) cloud computing services, which it provides to agencies across the federal government, including the Food and Drug Administration, the Centers for Disease Control and Prevention, the State Department, and NASA. The largest and most headline-grabbing contract was awarded to AWS by the Central Intelligence Agency (CIA) in 2013, a massive, $600 million contract to provide secure cloud services to the CIA and the rest of the intelligence community.

The secure cloud program for the CIA, known as Commercial Cloud Services (C2S) promised tailor-made data storage, processing, and analysis services across all levels of classification, as well as similar services to all 17 federal intelligence agencies in a "secret region," up to the secret classification level.[xi] It also promised significant cost savings to the intelligence community, because each agency would pay only for the services that agency needed.

While AWS began offering cloud services to government agencies in 2006, Frank Konkel, executive editor of Nextgov, told Open the Government that the 2013 CIA contract was the real breakthrough for Amazon. "It validated the technology…because if it's safe enough for the CIA, it should be safe enough for the rest of government." In 2014, the Obama administration chose to run its "cloud.gov", a service to help agencies transition to cloud services, on AWS. Konkel explained that now there is hardly any government agency that doesn't use AWS cloud services in some way. Even when AWS is not the direct provider, it's often partnered with other contractors. In 2013, half of the ten vendors that were part of a $10 billion Interior Department contract partnered with Amazon.[xii]



Jeff Bezos
@JeffBezos

A pleasure to host #SecDef James Mattis at Amazon HQ in Seattle today

1:31 PM - 10 Aug 2017

1,343 Retweets 5,679 Likes

770 1.3K 5.7K

Jeff Bezos
@JeffBezos
Amazon, Blue Origin, Washington Post
Joined July 2008

© 2019 Twitter About
Privacy policy Cook

Jeff Bezos Tweet.

The CIA has continued praising AWS in the years since C2S began operating. CIA CIO John Edwards called C2S "the best decision we've ever made," and another top CIA tech official called it "transformational."[xiii] This work, and the praise from the CIA, has helped make Amazon the frontrunner for what may be the largest government IT contract in history - the Pentagon's Joint Enterprise Defense Infrastructure (JEDI) program.

The shadowy war for the JEDI contract

The JEDI program will be similar to C2S-common cloud architecture across DoD. The project will be worth up to $10 billion over its full ten-year contract, and Amazon is widely expected to win based largely on its previous work for the CIA and the intelligence community. Defense One technology editor Patrick Tucker explained that in 2017, then-Defense Secretary Mattis took a trip to visit Amazon and Google headquarters, and came back convinced that DoD needed a common cloud to facilitate AI development-his true interest. “It seemed that there were only two companies who could do it-Amazon and Google,” Tucker said, “and Microsoft emerged later as a third.” Google later withdrew from the competition, and now Amazon and Microsoft are generally considered the only two companies left in the running, with Amazon the clear frontrunner.

Modern server room in datacenter. iStock/Getty Images

That doesn’t mean its competitors are going down without a fight.

In particular, Amazon rivals IBM and Oracle have criticized the Pentagon’s decision to choose a single provider for the contract, on the grounds that this contract formulation was tailored to Amazon. Choosing just one provider for such a large swath of the Pentagon’s cloud computing also raises concerns that DoD could become “locked in” to a single vendor, forcing the agency to continue buying services from that one vendor and essentially creating a monopoly. But DoD has stood firm, arguing that dividing JEDI up among multiple cloud service providers would slow down the project and weaken data-sharing capabilities across the agency.[xiv]

Oracle also challenged DoD’s decision to hand a separate, nearly $1 billion-contract to REAN, a Herndon, Virginia-based cloud provider and partner of Amazon Web Services. Oracle protested the award with the Government Accountability Office, and eventually DoD reduced the award from $950 million to just $65 million.[xv] Still, the award to an AWS partner was enough to convince Amazon’s competitors that the company had an unfair advantage in the bidding for the larger JEDI contract. When Amazon won the 2013 contract with the CIA, IBM protested that award as well, on the grounds that it had offered a lower bid than Amazon. GAO ruled against IBM, however, finding that Amazon had offered the CIA better technical solutions, making up for the difference in price.[xvi]

Many see the protests from companies like Oracle and IBM as a desperate attempt from the old guard of government IT contractors to preserve their dominance in the space against new competitors like Amazon and Google. Indeed, over the past five years Amazon has taken Washington by storm, more than quadrupling its lobbying expenditures in Washington-a far greater increase than any of its competitors over the same period.[xvii]

All that lobbying seems to be paying off. In 2017, Amazon fought for a procurement reform provision in the National Defense Authorization Act that would allow DoD to set up an online portal for acquisition of commercial products. Congress passed the so-called "Amazon amendment" as part of the final bill, and critics say that the specifications are such that only large companies like Amazon and Walmart could realistically compete for the contracts.[xviii]

Absent transparency requirements, a growing tide of tech workers are turning into whistleblowers to expose serious ethical abuse and human rights violations as they occur

While we know some about Amazon's lobbying of Congress, American University professor James Thurber explained that the public knows very little about how companies advocate for contracts with executive branch agencies. Individuals in the private sector who lobby Congress must register as lobbyists and file quarterly reports on their lobbying activities, but the same rules do not apply to those advocating in DoD or other agencies on behalf of their employers. It's therefore very difficult for the public to know how the companies vying for the JEDI contract have been working to sway the Pentagon's decision. "We should be extending the requirements in the Lobbying Disclosure Act to people influencing procurement and lobbying the executive branch," Thurber said, "and requiring them to register as lobbyists."

Even that wouldn't touch the problem of the revolving door of federal employees who leave government to work in the private sector, and vice versa. Federal appointees who enter government after lobbying face a two-year ban from working on the same issues on which they lobbied, but this doesn't necessarily prevent them from working on different projects that affect their previous employer.[xix] "There are rules," Thurber said, "but there are ways to get around them."

Indeed, Amazon seems to have exploited one such loophole, and now Amazon competitor Oracle is suing DoD over alleged ethics violations. The suit claims that the JEDI contracting process was rigged in Amazon's favor as a result of the Pentagon's revolving door. As part of the suit, Oracle is accusing DoD of allowing two former AWS employees to take part in shaping the contract, giving them the ability to tailor it to Amazon's exact capabilities. One of those employees, Deap Ubhi, had worked at Amazon before joining DoD in 2016 to work on the JEDI contract, and then rejoined Amazon shortly after leaving DoD in 2017.[xx] The Pentagon said that Ubhi did not significantly influence the development of the contract.[xxi]

The other DoD official implicated in the Oracle lawsuit is Anthony DeMartino, who was an Amazon consultant before becoming chief of staff to then-Deputy Secretary of Defense and now-Acting Defense Secretary Patrick Shanahan. Oracle alleges that the DoD's Standards of

Conduct Office advised DeMartino not to participate in the JEDI contract, but that it was his boss Shanahan who led the JEDI procurement process. In February, the Federal Claims Court issued a stay in the case so that DoD could thoroughly investigate potential conflicts of interest, threatening to delay the JEDI award, which is currently set for April.[xxii]

An important caveat to the allegations against Amazon is that most come from its competitors. A secretive dossier shopped around to media outlets contained even more sensational allegations about Amazon's DoD connections, including information about supposed romantic relationships, tenuous social media connections, and more.[xxiii] A private investigations firm shopped around the dossier, but it is widely speculated that it was paid for by Amazon competitors. Tucker, one of the journalists who saw the dossier, described it as "riddled with errors." It's also likely that, given the serious problem of contractor capture at the Pentagon, the other companies competing for JEDI may also be implicated in conflicts of interest at the agency.[xxiv]

And then there is HQ2. As previously noted, when Amazon announced that one of its two new headquarters locations would be in Arlington, Virginia, speculation arose that the decision had much to do with Amazon's competition for JEDI. Although Virginia gave Amazon a $750 million subsidy for its HQ2 site in Arlington, it's likely that Amazon had more than subsidies in mind when it chose a location so close to the Pentagon. The proximity to Washington can't hurt Amazon's chances at winning the JEDI contract, and HQ2 just happens to be landing in Crystal City, the Northern Virginia neighborhood that's also home to DoD's newly-formed Joint Artificial Intelligence Center.

Two members of Congress, Rep. Tom Cole (R-OK) and Rep. Steve Womack (R-AR) wrote a letter to the Pentagon Inspector General in October requesting an IG review of the JEDI contract process.[xxv] In March, Federal News Network reported that the Pentagon IG and the FBI's Public Corruption Squad are investigating the JEDI contract process.[xxvi]

A dark and ominous "cloud"

The government has fallen well behind the private sector in terms of transitioning to cloud technology, but it's trying to catch up. "Cloud is becoming perhaps the most important backbone technology in government," Konkel of NextGov told OTG. "It's being used to provide a variety of important government services…It's becoming ubiquitous." While many of us are used to thinking of the "cloud" as simple data storage, the government's interest in the technology goes much farther-particularly in the defense and national security sectors.

These computing capabilities facilitate AI and machine learning, which DoD says will "support lethality and enhanced operational efficiency"

One of the primary reasons that DoD is investing so much in the JEDI contract is outlined in the agency's cloud strategy released in February.[xxvii] The strategy document explains that the agency's current cloud set-up necessitates that its data be stored across multiple clouds in different DoD components. Instead, DoD believes that its data must be held in one common, agency-wide cloud that will both make the data more secure and - crucially - enable advances in artificial intelligence (AI) and machine learning.

The cloud, the strategy document explains, will enhance computing capabilities, allowing DoD data to be processed and analyzed at much greater speed. These computing capabilities facilitate AI and machine learning, which DoD says will "support lethality and enhanced operational efficiency."[xxviii]

The CIA has also made clear that big data analysis, machine learning, and AI algorithms are a crucial part of how the agency is using C2S, but has provided very little information about what those capabilities are used for. The FBI, too, is investing in AI technology. In addition to piloting Amazon's Rekognition facial recognition software, the agency is also employing AWS analysis services in counterterrorism investigations.[xxix]

The focus on AI is not surprising, given that experts have consistently warned that Russia, China, and other nations are making AI advances of their own. Because AI is useful across all sectors and industries and largely being developed by the private sector, the coming AI arms race will likely see some smaller countries emerge as leaders in addition to larger countries like the United States.[xxx] On February 11, President Trump issued an Executive Order aimed at keeping the U.S. ahead of the international curve, which promised to invest significant federal resources in research and development and in recruiting top talent.[xxxi]

Intelligence Air Force Illustration. Sgt. Alexandre Montes/DoD

The boost to AI infrastructure will be a welcome one, but the danger is that oversight and accountability mechanisms have not caught up with the burgeoning technology. Both the Executive Order as well as the first DoD AI strategy, released February 12, make commitments to improving public access to government data and AI processes.[xxxii] However, information about which AI capabilities are being employed by the federal government is currently woefully opaque, even more so for the DoD, CIA, and other national security agencies.

Machine learning on the battlefield and at home

Under a 2012 DoD directive, the military has forbidden itself from using completely autonomous weapons systems in combat-in other words, there must always be a human supervising and ready to intervene when an autonomous system is deployed.[xxxiii] In addition, the directive forbids the use of autonomous and semi-autonomous systems to engage human targets.[xxxiv] However, DoD has been using weapons with varying degrees of autonomy and reliance on AI algorithms for years. In fact, the first operational fully autonomous weapon was the Tomahawk Anti-Ship Missile (TASM), deployed by the U.S. Navy in the 1980s to search for and fire on Soviet ships on its own, though it was never fired in combat.[xxxv] Still, use of autonomous and semi-autonomous weapons remains exceedingly rare for a multitude of reasons, and those that are used today are a far cry from possessing human-level complex intelligence, or from the threatening prospect of the "killer robot." But such technology is on the horizon.

The military's uses of and ambitions for AI range from target identification to intelligence analysis, predictive maintenance, cybersecurity, and a whole host of logistical functions. The Pentagon has also indicated, via research the agency is funding at universities, an interest in using AI to predict protests and social unrest both abroad and domestically.[xxxvi] Potential future uses include major changes to military strategy and decision-making facilitated by AI-fueled data analysis.[xxxvii] And while the 2012 directive prevents the use of autonomous weapons systems to target humans, many of these current and future non-kinetic uses of AI will inform and contribute to lethal attacks on humans.

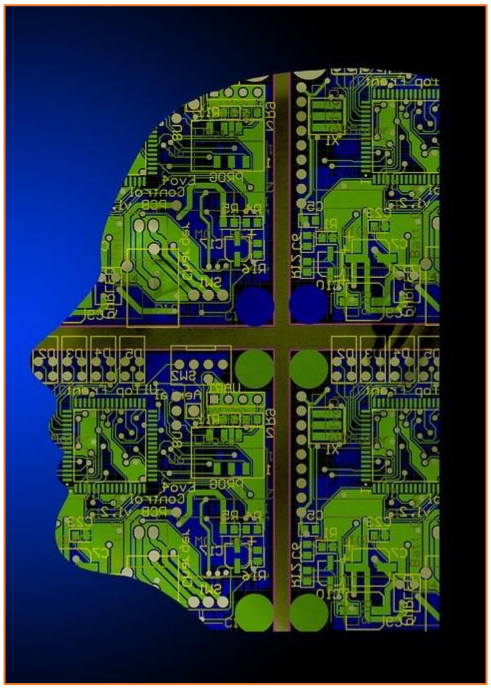
DoD's Project Maven, for example, has already used AI algorithms to search surveillance footage for beneficial intelligence, information that the military used to select targets to engage in airstrikes in Iraq and Syria.[xxxviii] Project Maven made headlines last year when Google employees protested the company's involvement in the DoD project. Some employees resigned in protest, while thousands of others signed a petition demanding that Google cancel their Project Maven contract. Ultimately, Google announced that it would not renew the contract once it ended, and that it would release a set of principles guiding its future AI work.[xxxix]

Many of these current and future non-kinetic uses of AI will inform and contribute to lethal attacks on humans

We know even less about the CIA's use of AI and AWS services. CIA tech official Steve Roche discussed using complex machine learning, or deep learning, to create "digital signatures" for individuals by analyzing the intelligence community's existing big data.[xl] Between them, Amazon and the intelligence community have amassed an enormous amount of individuals' personal data, a stockpile that is increasing all the time. Amazon recently purchased router company Eero, stoking fears that it will soon gobble up even more data on individuals' internet usage.[xli] While Amazon joins other major tech companies in publishing transparency reports with information about how frequently the government requests customer data, Amazon's reports are meager compared to its peers and the company refuses to publish data on how often it hands over data on home devices like the Amazon Echo.[xlii]

The Trump administration has also revived the CIA drone strike program, through which the agency is conducting an unknown number of airstrikes in secret, and the public is left in the dark as to whether the agency is using technology similar to DoD's Project Maven.

I’m working on *what*?



Artificial Intelligence. Courtesy of Pixabay

The set of principles Google released following the Project Maven controversy emphasizes the importance of avoiding bias in AI, testing systems for safety, and incorporating privacy protections, while committing to not allow the technology to be used for “weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people.”[xliii] Purportedly in accordance with these principles, Google withdrew from consideration for the JEDI contract, but did not rule out future collaboration with the military.

After the fact, The Intercept reported that not only had Google initially attempted to hide its Project Maven contract from employees (employee backlash started when Gizmodo revealed the contract), but that it had also hired additional workers to contribute to the project via a crowdsourcing website without telling them they were working on Maven.[xliv] The incident sparks concerns that future tech workers might also contribute to projects they find ethically questionable without their knowledge and consent.

Other companies refused to follow Google’s lead in backtracking from selling AI services to the military. Despite facing their own employee protests regarding ICE use of their AI technologies, Microsoft and Amazon declared their continuing intent to work with the military and law enforcement.[xlv] Teresa Carlson, a vice president at AWS, told the audience at the 2018 Aspen Security Forum that Amazon has “not drawn any lines” in terms of the government’s use of its technology, despite the fact that the company “doesn’t know everything they’re actually utilizing the tool for.”[xlvi]

In October, Microsoft also reaffirmed its willingness to sell AI and whatever other technologies the military and intelligence community desire, and Microsoft is currently considered to be the only other company with a shot at winning the JEDI contract. Microsoft president Brad Smith expressed his belief that selling AI to the military and intelligence agencies would allow the company “to engage in the public debate about how new technologies can best be used in a responsible way.” Still, he acknowledged that “we can’t control how the U.S. military uses our technology once we give it to them.”[xlvii] Microsoft has continued to receive pushback from employees. In February, a group of Microsoft employees wrote a letter stating their objections to providing augmented reality technology to the military. The employees wrote that the technology crosses the line into weapons development, because “it will be deployed on the battlefield, and works by turning warfare into a simulated 'video game.'" The employees also noted that, while Microsoft has an AI ethics review process, it is "opaque," and that "Microsoft fails to inform its engineers on the intent of the software they are building," further fueling fears that tech companies may not adequately inform their employees about the projects they're working on.[xlviii]

New York Times journalist Kevin Roose offered a cautionary tale for technology companies considering contracting with the military. Dow Chemical saw its public image transform from the manufacturer of household plastics to an enabler of war crimes when it started providing Napalm to the military during the Vietnam War. When news outlets started showing images of Vietnamese children with horrific burns, activists targeted Dow Chemical with protests. It took decades and likely billions of dollars in public relations campaigns for the company to restore its image.[xlix]

For its part, the DoD has also said it will create a set of ethics and principles governing its use of AI. In the AI strategy the Pentagon released in February, the agency committed to developing adequate testing and evaluation of AI systems, using AI to reduce civilian harm in armed conflicts, and advocating for global AI guidelines.[l]

The machine has a mind of its own

Despite these stated intentions, it is not clear that it is technologically possible to fulfill them in AI's current form. The more complex the algorithms involved in an AI system, the more opaque the analysis the computer is making and the more difficult it is for anyone, including the system's human creators, to discern what went in to the answer the computer spits out. Confusingly, some experts refer to the technology as "transparent," but what they mean in the case of AI is that "integration [of algorithms] into a product is not immediately recognizable."[li] In other words, it's very difficult even to tell that AI is at work in a given weapons system, much less how an algorithm is functioning.

> ***[Amazon] has "not drawn any lines" in terms of the government's use of its technology, despite the fact that the company "doesn't know everything they're actually utilizing the tool for"***
>
> ***- Teresa Carlson, vice president, AWS***

A group of researchers studying AI in 2017 for potential use by DoD found that "…it is not clear that the existing AI paradigm is immediately amenable to any sort of software engineering validation and verification." That is, adequate testing and evaluation to ensure that complex AI systems behave predictably in all possible situations may not currently be feasible. The researchers went on to state, "this is a serious issue, and is a potential roadblock to DoD's use of these modern AI systems, especially when considering the liability and accountability of using AI in lethal systems."[lii] According to the Congressional Research Service, "perhaps the most immediate policy concern among AI analysts is the absence of an independent entity to develop and enforce AI safety standards and to oversee government-wide AI research."[liii]

In his 2018 book, AI expert Paul Scharre contrasted a potential failure of an AI system to the nuclear accident at Three Mile Island. "The accident at Three Mile Island might not have been predictable ahead of time," Scharre wrote, "but it is at least understandable after the fact."[liv] Even the most expert officials might not be able to determine how an AI system failed. DoD may intend to make AI more "explainable"-allowing experts to understand how a computer made its decision-and develop testing and evaluation methods, but it may not be possible at the current state of AI development. According to CRS, "AI systems do not [currently] have an audit trail for the military test community to certify that a system is meeting performance standards."[lv]

> ***"The susceptibility of complex AI systems to "adversarial images," or manipulated images containing spoofing attack…could be fed to the AI system without the human supervising the system being able to tell that the image had been changed at all"***
>
> ***- Jeff Clune, AI researcher, University of Wisconsin***

There are also serious vulnerabilities exacerbated by the opacity of complex machine learning. Jeff Clune, an AI researcher at the University of Wyoming, told Scharre about the susceptibility of complex AI systems to "adversarial images," or manipulated images containing spoofing attacks that could be fed to the AI system without the human supervising the system being able to tell that the image had been changed at all.[lvi] Such vulnerabilities are particularly dangerous if used to inform lethal military attacks. In such an instance, even a human receiving the information from the AI system would likely not be able to tell that the intelligence was faulty. Even with simpler AI systems, vulnerability to hacking is a major problem. In 2017, a small AI startup Clarifai, was hacked by "one or more people in Russia, potentially exposing technology used by the U.S. government to an adversary." Clarifai uses AWS infrastructure for its AI software, and the credentials to Clarifai's AWS account were compromised in the attack.[lvii]

> ***Vulnerability to hacking is a major problem. One of the small contractors working on Project Maven was hacked in 2017***

Researchers from Technology For Global Security and the Center for Global Security have also noted the possibility that increased reliance on machine learning and AI could lead to major changes in strategic decisions related to war and armed conflict. The researchers argue that "AI may be seen as eroding mutual strategic vulnerability and thereby as increasing the risk of war" by changing the strategic calculus and making preemptive strikes a more appealing option.[lviii]

Currently, deep machine learning is still in the "research phase" for DoD, according to Defense One's Tucker. However, the Pentagon's Defense Innovation Board states on its website that "the impact of AI and ML will be felt in every corner of the Department's operations, from critical tactical operations such as Intelligence, Surveillance, and Reconnaissance (ISR), targeting…and threat analysis and war-gaming."[lix] All signs point to DoD seeking to develop complex machine learning systems for operational use, ensuring that these issues will become more important in the coming years.

Finally, it stands to reason that concerns about inherent bias would apply to the use of algorithms in national security and counterterrorism programs as well as those used in law enforcement. If the military and intelligence agencies are using face and voice recognition programs, they would be susceptible to the same biases as Amazon's Rekognition software and other similar programs. (Read more about Rekognition's bias and accuracy problems in Part Two of this report.)

The black box

The public does not know which computing services and AI capabilities AWS is providing to the intelligence community, nor do we know the services and capabilities promised to DoD as part of the JEDI contract. This secrecy is compounded by other systemic factors that further prevent adequate oversight and accountability in the use of these technologies.

"The impact of Artificial Intelligence and Machine Learning will be felt in every corner of the Department's operations
- Department of Defense website

First, it's important to note that the mere fact this work is being carried out largely by private contractors presents a serious barrier to public access to information. Government contractors like Amazon are not subject to the Freedom of Information Act (FOIA), and there is an exemption built into the law that prevents information deemed to be trade secrets from being released to a FOIA requester. As a result, the more that government services are being provided by private contractors, the less ability the public has to access documents related to that work.

Yahoo News reporter Jenna McLaughlin underscored the problem: "I'd love to be able to FOIA Amazon for what they're doing with the CIA," she told OTG, "and to have the ability to understand what contractors are doing and what technology they're providing. You have a situation now where private contractors are often working side-by-side with intelligence officials, and it's harder to discern between government and private sector." McLaughlin worked on a 2018 investigation into a major failure in a CIA communications system that resulted in the imprisonment or death of dozens of CIA sources. Contractors were deeply involved in the system, and one source told McLaughlin and fellow reporter Zach Dorfman that the government "'keeps paying shitty defense contractors' to work on covert communications."[lx] And while the private and public workforces may be becoming more integrated, that doesn't necessarily translate into transparency between them.

The more that government services are being provided by private contractors, the less ability the public has to access documents related to that work.

Clarifai, the startup that was hacked while working on Project Maven, was sued by a former employee who alleges that she was fired for criticizing the company's failure to promptly disclose the breach to the Pentagon.[lxi]

Decreasing transparency in the procurement process is another possible consequence of growing reliance on private contractors to develop new technologies. DoD is increasing its use of "other transaction agreements" (OTA's) instead of normal procurement contracts, allegedly in order to bypass bureaucratic requirements that slow down acquisition and discourage the private sector from working with federal agencies. OTA's are used by the government to fund research, prototyping, and production of new technology by private companies, and were intended to encourage nontraditional providers to enter the government contracting space. However, OTA's also "remove many taxpayer and transparency protections," according to Project On Government Oversight general counsel Scott Amey. Amey explained that without the requirements of normal procurements, it's difficult to know much of anything about OTA's and whether they're truly going to nontraditional companies, or merely providing the traditional providers with a way to get around competition and cost and pricing regulations that protect agencies. In its decision against the cloud contract that went to AWS partner REAN, GAO found that DoD had improperly used an OTA when it could have used a normal, competitive contract.[lxii] The Microsoft contract to provide augmented reality technology to the military that came under fire from Microsoft employees is also an OTA.[lxiii]

Private contractors are often working side-by-side with intelligence officials, and it's harder to discern between government and private sector.

Furthermore, while the defense and national security agencies are already rife with overclassification, this new surge in AI development and implementation comes at a time of diminishing transparency at the Pentagon.[lxiv] At the same time DoD is relying on Project Maven AI to assist in airstrike targeting in Iraq and Syria, the agency has stopped releasing a significant amount of information about U.S. airstrikes in those countries. Over the course of 2018, the timeframe that DoD began utilizing algorithms to help identify targets for strikes, U.S.-led coalition airstrikes killed an estimated 821 to 1,712 civilians in Iraq and Syria.[lxv] Despite an additional surge in airstrikes in late December, the Pentagon stopped publicly releasing information on the targets and dates of strikes, with little explanation.[lxvi] Without knowing even this basic information about U.S. air strikes, how can the public, or Congressional overseers, discern whether or not there was an error in the computer's analysis of drone footage or whether the system was hacked? Who is accountable if an algorithm fails and civilians are killed?

Without knowing even this basic information about U.S. air strikes, how can the public, or Congressional overseers, discern whether or not there was an error in the computer's analysis of drone footage or whether the system was hacked? Who is accountable if an algorithm fails and civilians are killed?

We don’t know whether the use of this technology has expanded to battlefields beyond Iraq and Syria, but we do know that DoD considers Project Maven to be a success and is interested in emulating it. DoD’s new Joint Artificial Intelligence Center (JAIC) will be led by Project Maven head Lt. Gen. Jack Shanahan. As AI expert Scharre told Defense One, “The JAIC is, in many ways, an expansion of what Maven started, with the aim of scaling up a project into an institution that can help bring AI technology into the Department as a whole.”[lxvii]

If the technology is being used in the drone program, at either DoD or the CIA, the risks only increase. The practice of “signature strikes,” or targeting individuals for lethal drone strikes based on patterns of behavior rather than identity, first came to light during the Obama administration and invoked sharp criticisms from human rights groups.[lxviii] Under the Trump administration, the practice has most likely continued and possibly even expanded, all with no transparency from the White House on what changes have been made to the rules governing the drone program.[lxix] The danger of policies like these could be exacerbated by introducing AI into that process. “If there’s a fundamental flaw in the way you’re collecting intelligence or running a program,” Defense One’s Tucker told OTG, “then AI will just accelerate a bad practice.”

In 2017, the Institute of Electrical and Electronics Engineers (IEEE) released its own “vision for prioritizing human well-being” in AI via its Global Initiative on Ethics of Autonomous and Intelligent Systems. The document notes that accountability and transparency are two areas of concern that go hand-in-hand. “Lack of transparency,” it reads, “both increases the risk and magnitude of harm (users not understanding the systems they are using) and also increases the difficulty of ensuring accountability.”[lxx]

One specific way in which secrecy stands in the way of accountability is by inhibiting Congressional oversight. If Congressional oversight committees do not have access to information about whether and how AI and machine learning systems fail or are misused, they have no way to hold agencies accountable for any resulting harm or waste. Another issue is that Congressional offices, whose ranks are filled with policy analysts and lawyers, may not have staff with adequate technological expertise, as well as the requisite security clearances to oversee DOD and the intelligence community. “I do not necessarily think that Congress is well-equipped to understand these technologies,” McLaughlin told OTG, “and Congress always has problems recruiting, because they aren’t able to pay as well as the private sector.”

> ***“If there’s a fundamental flaw in the way you’re collecting intelligence or running a program then AI will just accelerate a bad idea”***
>
> ***- Patrick Tucker, Defense One***

Part 2: The private side of public security

In October 2018, hundreds of Amazon employees publicly called for CEO Jeff Bezos and other executives to stop selling surveillance tools to government agencies. Employees said they "refuse to contribute to tools that violate human rights," citing abuses by ICE and police targeting of activists.[lxxi] At the heart of the controversy is Amazon's facial recognition system, Rekognition. The product, powered by Amazon Web Services (AWS), uses artificial intelligence to identify, track and analyze people in real time, and quickly scan information against databases containing tens of millions of faces.[lxxii] "We can sell dangerous surveillance systems to police or we can stand up for what's right," the employees said. "We can't do both."[lxxiii]

The outcry from Amazon employees followed a series of revelations made possible through public records requests that provide a glimpse of how deeply imbedded Amazon's technology is in security enforcement.[lxxiv] Nevertheless, the extent to which the government relies on Amazon is anyone's guess. We do not know all the security enforcement agencies using AWS or Rekognition. Safeguards to prevent police from using the technology to secretly spy on citizens and non-citizens alike are either weak or non-existent. Broad exemptions to transparency laws, nondisclosure agreements and lack of public notice requirements keep communities from knowing when and how the technology is used. Even Amazon shareholders say that Rekognition could be used to "unfairly and disproportionately target and surveil people of color, immigrants, and civil society organizations," warning that "…sales may be expanded to foreign governments, including authoritarian regimes."[lxxv] Yet the secrecy makes it difficult to understand the social impacts and systematic violations of First and Fourth Amendment protections.

"We can sell dangerous surveillance systems to police or we can stand up for what's right. We can't do both"

- Amazon Employees

The controversial technology is not unique to Amazon. A growing number of companies are competing to sell artificial intelligence tools such as facial recognition and image-scanning to government agencies. Microsoft is leading the development of facial recognition technology, and a crop of startups sell software that scans people's faces for marketing purposes. Most companies advertise real-time face recognition systems, which are associated with the highest threats to privacy.[lxxvi] Law enforcement across the country is adopting the technology, and facial recognition is becoming ubiquitous in public areas, including airports, schools, and protest spaces.[lxxvii]

Objections from Silicon Valley workers have grown under the Trump administration. As noted in Part 1, Google and Microsoft both faced employee objections to the companies' decision to contract with the DoD. Digital rights advocates have launched a campaign making it easier for employees at the largest tech companies to blow the whistle on unethical uses of technology.[lxxviii]

Rekognition "could be used to "unfairly and disproportionately target and surveil people of color, immigrants, and civil society organizations…sales may be expanded to foreign governments, including authoritarian regimes"

- Amazon Shareholders

Amazon, however, has garnered a large share of the attention, due in part to its domination of the market of easy-to-use and affordable surveillance technology, and its unwavering support for law enforcement, defense and intelligence agencies.[lxxix] While the large part of Amazon's operations remain clouded in secrecy, journalists, investigators, and advocates have exposed evidence of government overreach and abuse associated with Amazon's products. The investigations illuminate how the spread of invasive technology is moving faster than the public knows and than policymakers can regulate.

Computers and cages

In June 2018, as outrage grew over children being torn away from their parents at the border, attention shifted towards the private contractors profiting from the effort.[lxxx] The protest from tech workers grew, as more employees objected to providing services that facilitated the separation, detention, and deportation of immigrants. In the face of the "increasingly inhumane treatment of refugees and immigrants beyond this specific policy," Amazon employees wrote, "we are deeply concerned that Amazon is implicated, providing infrastructure and services that enable ICE and DHS."[lxxxi]

Children in a detention facility in McAllen, Texas. U.S. Customs and Border Protection

Employees with Salesforce wrote to CEO Marc Benioff, demanding the company "re-examine" its relationship with the Customs and Border Protection (CBP), and cut any contracts with the agency.[lxxxii] Microsoft employees called on the company to cancel its $19.4 million cloud-computing deal that provides artificial intelligence capabilities to ICE.[lxxxiii] The letter requested Microsoft draft, "publicize, and enforce a clear policy stating that neither Microsoft nor its contractors will work with clients who violate international human rights law," and to "commit to transparency and review regarding contracts between Microsoft and government agencies, in the U.S. and beyond."[lxxxiv]

In response, Microsoft CEO Satya Nadella downplayed Microsoft's work with ICE, claiming the company merely provides the agency with routine tech services like email, calendar, and messaging.[lxxxv] The statement appears to contradict a January 2018 blog post, however, in which Microsoft said it was proud to work with ICE and provide the agency "deep learning capabilities to accelerate facial recognition and identification."[lxxxvi] Nadella called the family separation policy "cruel and abusive," but would not commit to canceling contracts with ICE, as requested by the employees.

Sayta Nadella, Microsoft CEO. Wikimedia Commons

The objections from tech workers highlight concerns that the country's biggest companies are facilitating the Trump administration's anti-immigrant policies. Contractors provide the software used in the web of sweeping surveillance that funnels separated families, refugee seekers, Dreamers, Temporary Protected Status holders, visa holders, lawful citizens and entire immigrant communities into the deportation machine. Further, the government's increased privatization of immigration enforcement creates a major impediment for effective oversight and accountability. The Obama administration established surveillance programs targeting undocumented communities that created many of the current obstacles to understanding the private actors behind today's enforcement apparatus.[lxxxvii] Building on that foundation, the Trump administration increasingly uses opaque information systems in ways that disproportionately threaten marginalized communities and violate due process.[lxxxviii]

Immigrants caught in web of public-private partnerships

The intersection of tech companies and the immigration enforcement infrastructure undermines legal protections to privacy, freedom of association, free speech and due process.[lxxxix] Accelerated surveillance technology allows ICE to bypass local and state laws intended to protect marginalized communities from discriminatory policing. Local governments that pass sanctuary city laws, for example, are helpless to stop federal authorities from accessing data and illegally targeting undocumented communities.

Companies that profit from the administration's immigration enforcement polices by supplying the government with secretive technology include Microsoft, Akamai, Oracle, IBM, Google, Palantir, and others. [xc]

Surveillance. iStock/Getty Images

However, Amazon is the big winner. As the biggest provider of cloud storage for the government, Amazon profits from the administration's anti-immigrant crackdown. ICE's Investigative Case Management (ICM) system, CBP's Biometric Entry-Exit program, DHS's biometric databases, and an information-sharing platform with Mexico are all powered by AWS.[xci] Amazon has also come under fire for selling its services to companies such as Palantir-the data analytics firm co-founded by billionaire investor Peter Thiel, who served as an advisor on President Trump's transition team.[xcii] Palantir started with funding from the CIA's venture capital arm In-Q-Tel, and its client list has grown to include Department of Homeland Security, Federal Bureau of Investigations, National Security Agency, Centers for Disease Control, Marine Corps, Air Force, Special Operations Command, West Point and the Internal Revenue Service.[xciii] Palantir's influence in government has also grown through revolving door appointments of former lobbyists now in influential government policymaking positions.[xciv]

Palantir sells software to police departments and federal agencies, connecting a web of databases that are difficult to track and largely unaccountable.[xcv] The company designed ICE's aforementioned case management system, which pulls data from an array of federal law enforcement and private databases to profile immigrant communities, and track, detain and deport individuals.[xcvi] Palantir has a $51 million contract with ICE, and pays Amazon around $600,000 a month to use its servers. Compared to other companies, Amazon has an advantage when it comes to securing such highly lucrative contracts.[xcvii] IT systems like ICM must be hosted on federally authorized cloud services, and Amazon receives the largest share of federal authorizations for storing, processing and transmitting government data.[xcviii] Because of the direct connection to the administration's deportation operations, Amazon employees called on the company to stop selling AWS to Palantir specifically.[xcix]

Agents arrest a suspect/Photo Courtesy of ICE

"Amazon's decision to continue selling AWS is demonstrative of Silicon Valley's reckless approach to expanding the government's technological infrastructure," Paromita Shah, Associate Director of the National Immigration Project of the National Lawyers Guild, told OTG. "We're seeing this technology increasingly weaponized, and it is deeply troubling that Amazon sells its services for immigration enforcement without considering the social impact. These companies can no longer pretend to ignore what's happening-they are willfully taking taxpayer's dollars to fuel the aggressive policing of communities of color and immigrants."

Despite reporting and in-depth investigations, there is still little transparency when it comes to the role of private companies in detentions and deportations. We know that private contractors provide the software for immigration enforcement databases that include mobile biometric devices, DMV records, license plate reader programs, gang databases, and more.[c] We also know that systems such as ICM draw from this web of data, known for inaccuracies and bias, exacerbating discriminatory enforcement practices.[ci] What we don't know is how often the use of these databases and AI systems leads to indiscriminate raids, mis-identifications, wrongful detentions, and other abuses. Gang databases are particularly notorious for unlawful collection of information, leading to the detention and deportation of innocent victims.[cii] The use of such databases also leads to an unknown number of U.S. citizens detained each year.[ciii] ICE stopped releasing data on those taken into custody in 2017, making it impossible to know how many citizens fall victim to the aggressive increase in arrests and deportations.[civ]

"Amazon's decision to continue selling AWS is demonstrative of Silicon Valley's reckless approach to expanding the government's technological infrastructure"

Paromita Shah, Associate Director of the National Immigration Project of the National Lawyers Guild

Tech companies facilitate the expansion of immigration enforcement, and their close relationships with federal agencies and lawmakers spurs this growth. DHS has adopted a "multi-cloud strategy," and Amazon is the primary contractor in the $6.8 billion "enterprise-wide migration" information technology project. Some lawmakers worked to form a public-private partnership and pass legislation to codify the federal government's "cloud first" policy. The Members of Congress involved in that initiative, including Representatives Darrell Issa (R-CA) and Gerald Connolly (D-VA) have received over $250,000 in contributions from Amazon and other tech companies that benefit from the cloud computing contracts.[cv] Amazon, meanwhile, has increased investment in lobbying, jumping to nearly $15 million in 2018, up from $3 million in 2013.[cvi]

Amazon shows no signs of putting the brakes on its support of the government's immigration system.[cvii] In October 2018, the Project on Government Oversight (POGO) obtained internal records through FOIA requests showing that Amazon was aggressively working to sell its face recognition software directly to ICE.[cviii] Facial recognition technology in the hands of ICE's Enforcement and Removal Operations (ERO) could lead to constant automated surveillance of public spaces patronized by undocumented immigrants. Surveillance of sensitive locations like medical facilities, places of worship, and schools could discourage people from seeking out vital services for fear of being identified and detained. "If ICE gets their hands on facial recognition, it would exponentially increase the agency's ability to target and identify individuals, taking away from any prioritization in immigration enforcement," said Jake Laperruque, a Senior Counsel with POGO who filed the FOIA request for ICE records. "Turning ICE from an enforcement agency to a real-time surveillance apparatus is worrisome."

The meetings with ICE came after the public protests from Amazon employees and investors, indicating that the company does not intend to listen to the demands of its workers and shareholders.

Not your father's mugshot

Not wanting to limit itself to federal contracts, Amazon is also aggressively marketing face recognition software to police.[cix] Rekognition uses artificial intelligence to compare people captured in live or recorded footage against large databases which, according to the company's promotional materials, makes "investigation and monitoring of individuals easy and accurate."[cx] The enhanced surveillance power comes as more reports surface of police spying on Black Lives Matter activists and monitoring protests.[cxi] As OTG reported last year, the growth of constant surveillance along racial and political lines has a chilling effect on freedom of speech and protest organizing.[cxii]

Facial recognition software is enabling surveillance programs that could violate due process rights and disproportionately target communities of color without any legal recourse. Moreover, the technology is quietly spreading under the cover of nondisclosure agreements, with little oversight from lawmakers or the public.

The absence of federal laws or regulations governing the use of facial recognition amplifies civil rights concerns. Constitutional precedents on police use of facial recognition without a warrant do not exist, and courts have yet to decide whether facial recognition constitutes a search under the Fourth Amendment. As such, facial recognition software is enabling surveillance programs that could violate due process rights and disproportionately target communities of color without any legal recourse. Moreover, the technology is quietly spreading under the cover of nondisclosure agreements. with little oversight from lawmakers or the public.[cxiii] "The mentality of spy first, ask questions later is hugely problematic," POGO's Laperruque told OTG. "We have no idea just how much we don't know, and companies such as Amazon has been overly secretive about how their technology works."

After becoming a Rekognition customer in 2017, the sheriff's office of Washington County, Oregon, built a database of 300,000 mug shots of suspected criminals that officers scan against footage of potential suspects in real-time.[cxiv] The footage can come from public and private cameras as well as police body cameras, transforming body cameras from police accountability tools into mobile surveillance devices. According to internal documents, Amazon asked the county to tout its experience with Rekognition to other public sector customers, including a manufacturer of body cameras.[cxv] In response to public criticism, the sheriff's office said the goal of the program was "not mass surveillance or untargeted surveillance."[cxvi] However, Oregon police say they do not follow guidelines for matching suspects that Amazon recommends to its clients.[cxvii] Failing to use even baseline guidelines opens the door to widespread misidentifications, with innocent people potentially getting caught in the policing net.

"We are seeing ever increasing interest in using facial recognition for surveillance," says Clare Garvie, a senior associate at the Georgetown Law Center on Privacy and Technology. "Amazon's Rekognition pilot in places such as Orlando, Florida is one example of this technology being used for real-time scanning, which is associated with high risks to privacy and civil liberties," Garvie told OTG. Local advocates say that Orlando police started testing the program "without inviting a public debate, obtaining local legislative authorization, or adopting rules to prevent harm to Orlando community members."[cxviii] In an apparent win for privacy defenders, Orlando officials stopped using Rekognition in June 2018. However, they later said the decision was not due to the public criticism, and announced Orlando police would again renew a contract to pilot Rekognition.[cxix] Orlando officials appear poised to forge ahead, despite the fact that public records requests exposed a lack of hands-on training and flawed test results with the first pilot.[cxx]

"What makes facial recognition particularly invasive is that it can be done without your consent, done in secret, and done on a mass scale," Jeramie Scott, Senior Counsel and Director of the Electronic Privacy Information Center's Domestic Surveillance Project, told OTG. "The current environment allows for this type of technology to propagate without constraints, which has serious privacy implications. We need a more robust public debate, and should be discussing not only how we should be using the tech, but *if* we should be allowing the technology to be used at all [emphasis added]."

Real-time tracking by police enables law enforcement to identify groups of people, persons of interest, and patterns of movement, posing restrictions to freedom of speech and assembly. Studies find that people alter their behavior and associations in response to constant surveillance.[cxxi] Nonetheless, companies large and small are bolstering the secret spread of surveillance technology to police across the country. According to a Georgetown study co-authored by Garvie, at least a quarter of all law enforcement agencies have access to a facial recognition system.[cxxii] The rapid influx of new technology means that police are using personal data without regulations to protect from government overreach and abuse. In New York City, for example, IBM collaborated with the New York City Police Department to develop a face classification system from thousands of hours of NYPD surveillance footage that included "ethnicity search" as a custom feature.[cxxiii] It took a 2017 Congressional inquiry and freedom of information act requests to expose that police in Washington, D.C. used a facial recognition system that allowed law enforcement agents to query FBI databases without any federal policy guidelines in place.[cxxiv]

The acquisition of the technology is outpacing existing legal protections, and where some legal protections exist, the secret nature of facial recognition often allows for circumvention of the law. The FBI has failed to meet basic transparency requirements and conduct privacy assessments as mandated by federal law for its Next General Identification (NGI) database and its use of face recognition.[cxxv] The NGI database pulls from state and local databases, and provides access to criminal and personal data for more than 23,000 law enforcement agencies.[cxxvi] As more police departments acquire facial recognition technology, Americans increasingly become victims of privacy abuses as their personal information falls into the dark hole of government data sharing without their knowledge.

Open government proponents and civil rights defenders continue to call for greater transparency around the spread of face recognition technology, with a focus on Amazon. After months of employees calling for changes to the company's policies, however, an Amazon employee said in October 2018 the company had not given any official response to the internal letter, and there were no apparent changes in how it markets Rekognition.[cxxvii]

"At a time when we're having a serious debate about the use of invasive surveillance tech, it's troubling that companies are not listening to the demands of their concerned employees, and continue to aggressively sell to governments," Trevor Timm, Executive Director of the Freedom of the Press Foundation told OTG. "Silicon Valley workers have a unique insight into the threats posed by the spread of surveillance technology, and policymakers should be following their lead to address these threats."

Exacerbating the racial divide

Independent studies show problematic racial and gender inequities associated with facial recognition technology, illuminating the need for companies to address inherent bias and discrimination within the systems. Algorithms used by IBM and Microsoft correctly identified 99 percent of white men, but misidentified one out of three dark-skinned women, according to a February 2018 from MIT and Stanford researchers.[cxxviii] That study made headlines when the co-author from MIT, Joy Buolamwini, posted videos showing the technology misclassifying famous African-American women as men.[cxxix] As a graduate student, Buolamwini experienced first-hand the bias and exclusion that results from AI-powered facial detection. The robot she programmed for an assignment could not detect her dark-hued skin-she had to use her white roommate's face for the program to work.[cxxx] Even Microsoft admits that certain uses of facial recognition technology "increase the risk of decisions, outcomes and experiences that are biased and in violation of discrimination laws."[cxxxi] Criminal justice experts note that racially biased police practices in this country mean that criminal databases already include a disproportionate number of people of color.[cxxxii] Face recognition then exacerbates racial disparities by misidentifying minority groups at higher rates.

"When algorithms participate in the surveillance of public spaces and misidentify people of color or women, these communities are disproportionately at risk of getting caught in the criminal justice system," Deborah Raji, a University of Toronto researcher, told OTG. "The criminal justice system is already skewed along racial lines, and facial recognition tools are not calibrated to account for communities of color. That is a major social issue, in a country where the burden of being wrongly affiliated with a crime you were not involved in can be life altering."

Raji and Buolamwini released another study in January 2019 showing that Amazon's Rekognition software disproportionately misidentified female faces and darker-skinned individuals, performing even worse than similar services from IBM and Microsoft.[cxxxiii] The results generated national media attention, stoking more concerns over Amazon's aggressive efforts to expand sales of Rekognition.[cxxxiv]

Google said it would refrain from selling facial recognition products until the potential risks were addressed,[cxxxv] and Microsoft acknowledged the need to ensure the technology is not used in a harmful way.[cxxxvi] Amazon, however, downplayed evidence of potential biases in its technology, calling Raji and Boulamwini's study "misleading," and attacking the methodology.[cxxxvii] Responding to the dismissal, Buolamwini said that Amazon was missing the message: the company should be more diligent about checking *all* systems for potential bias.[cxxxviii]

"Our paper was designed to show where disparities exist in facial recognition programs, and provide a roadmap for future bias testing," Raji told OTG. "Our study used what shouldn't be a hard benchmark, and we tested a simple binary facial analysis task. Even in that case, Amazon still falls incredibly short. This means that there is an urgency for them to test their more complicated facial analysis systems, which are likely to perform even worse than those tested in our study."

A growing number of social scientists and policy experts express similar sentiments, warning that the spread of algorithmic decision-making worsens discrimination along socio-economic and racial divides.[cxxxix] AI Now, a group affiliated with New York University that includes employees of tech companies, has called for government regulations, stronger oversight, and greater transparency in the application of artificial intelligence software. The group argued in a December 2018 report for public notice to ensure consent from vulnerable communities.[cxl] The report specifically addresses concerns about Amazon's partnership with companies such as Palantir, using it as an example of how AI systems increase integration of surveillance technologies used as a mechanism of social control.[cxli]

"There is an urgency for [Amazon] to test their more complicated facial analysis systems, which are likely to perform even worse than those tested in our study"

- Deborah Raji, University of Toronto

"A major issue with AI systems is the way they channel public information into government decision-making," said Amie Stepanovich, Policy Manager with Access Now, an international digital rights organization: "There is a ton of unreliable and unsubstantiated data available online, which is accessed by companies, and then used by law enforcement and intelligence agencies. When government acquire this type of data directly, they are often bound by legal standards. With AI tools, however, this data may be swept up on a large scale with few safeguards in place. In a society where public data is more available than ever before, we need to control how it is used and analyzed by the government."

The law is lacking

"In a society where public data is more available than ever before, we need to control how it is used and analyzed by the government"

- Amie Stepanovich, Access Now

Despite documented issues of error and bias, federal regulation of the technology is lagging. Laws that do exist often serve to promote the use of facial recognition for surveillance.[cxlii] Some members of Congress are stepping up their oversight role and demanding answers. Members of the Congressional Black Caucus wrote Amazon's CEO in May 2018 expressing concern over the "profound negative unintended consequences," that the use of face recognition and artificial intelligence "could have for African Americans, undocumented immigrants, and protestors."[cxliii] Congressional interest grew dramatically after the ACLU released a study in July 2018 showing that Rekognition misidentified more than two dozen members of Congress as people arrested for crimes.[cxliv] The study showed serious racial disparity, with the error rate for non-white members of Congress 34 percent higher than Congress as a whole.[cxlv]

Senator Ed Markey (D-MA), Rep. Luis Gutierrez (D-IL) and Rep. Mark DeSaulnier (D-CA) sent a public letter to Amazon in July 2018 demanding information from the company.[cxlvi] The letter called for details about any internal bias assessments, lists of all law enforcement or intelligence agencies using Rekognition, assessments on whether the software was being used for secretive government surveillance, and additional information.[cxlvii] Separately, Rep. Jimmy Gomez (D-CA) urged Jeff Bezos to work with key stakeholders, communities of color, and policymakers, to create a policy and regulatory environment to keep up with the speed of technology.[cxlviii] Congress also called for the Government Accountability Office to evaluate the extent to which law enforcement agencies have public and transparent policies to prevent adverse impacts on privacy, civil rights, and civil liberties.[cxlix]

While waiting for that study, Members of Congress again wrote to Bezos in November 2018, requesting a response to unanswered questions.[cl] In February 2019, Rep. Gomez said Amazon still had not provided sufficient information, and called for the new Congress to hold a hearing and bring in company representatives to testify.[cli] The Chairman of the House Oversight and Affairs Committee, Rep. Elijah Cummings, said the Committee is currently considering investigating facial recognition and a hearing could be forthcoming.[clii]

The growing Congressional attention comes at a pivotal moment for determining the future of facial recognition use. Companies such as Microsoft have called for federal regulations, and policy experts have recommended what legislation should look like.[cliii] Faced with mounting pressure, Amazon finally came out in February 2019 in support of creating a regulatory framework, recommending that the technology comply with "all laws," including those that protect civil rights. Amazon's outline also suggested requiring regular transparency reports from law enforcement agencies on privacy safeguards, and calls for "sufficient notice" when video surveillance is deployed in public.[cliv] Yet Amazon also warned against banning or condemning the new technology "because of its potential misuse," signaling that the company would not wait for regulations to catch up while sales of Rekognition continued.[clv]

Until there is federal action, advocates are looking to lawmakers at the state and local level for protections against the spread of surveillance technologies. Proposals range from outright bans to regulations that would curb potential abuse. San Francisco lawmakers introduced legislation[clvi] in January 2019 that would make the city the first to ban government use of facial recognition software.[clvii] Massachusetts lawmakers have proposed a moratorium on face recognition and other biometric surveillance systems[clviii] and Washington State has proposed legislation to regulate the technology.[clix]

Some cities are also starting to take up legislation to ensure residents have maximum influence over decisions on whether and how local police use surveillance technologies in their communities.[clx] In the vast majority of cases, however, cities are acquiring surveillance technology without knowledge or consent of residents. Advocates and journalists rely on public records laws to uncover the technology, but secrecy agreements between companies and governments are often a major hurdle to transparency.

Part 3: Secrecy challenges: The fight for FOIA & the public's right to know

Public records laws help to expose the dangers associated with facial recognition and cloud-computing services. For every case of a successful disclosure, however, there are countless instances of potential abuse cloaked in secrecy. Nondisclosure agreements between companies and government entities aggravate the problem, restricting the public's right to know about the spread of the technology and its associated harms.

A document with redactions. iStock/Getty Images

At the federal level, agencies have denied FOIA requests for records on Amazon's cloud services, preventing the public and lawmakers from understanding the company's relationship with intelligence agencies. The CIA rejected a FOIA request in 2014 for information about Amazon's $600 million contract to provide cloud-computing services for the entire U.S. intelligence community.[clxi] BuzzFeed News senior investigative reporter, Jason Leopold, told OTG he has a four-year-old request pending with the CIA for a copy of the contract and records related to the discussions surrounding the agreement, but has not received any documents. The NSA denied a similar request in 2016 for records on that agency's contracts with Amazon, citing national security reasons.[clxii]

Immigration enforcement agencies regularly obstruct information requests and fail to comply with their FOIA obligations. Privacy groups are suing ICE to obtain records on Palantir's contracts with the agency, including records on the aforementioned ICM system.[clxiii] Paromita Shah, whose organization is suing ICE for records on biometrics data sharing, has warned against DHS having free reign to amass this kind of technology without a "serious public examination and discussion about its use, purpose, scale and design."[clxiv]

While the Project On Government Oversight was able to use FOIA to obtain emails confirming Amazon's efforts to sell its products to ICE, those emails were heavily redacted. POGO filed an appeal, and is waiting for additional records. ICE has delayed responding to and rejected requests filed by OTG for information on the surveillance of immigrant rights activists and information sharing agreements with police.[clxv] OTG and POGO's FOIA on the family separation policy revealed documents on the government's information management practices that were also heavily redacted, preventing the public from understanding whether private actors were involved in the flawed record keeping process.[clxvi] DHS is reviewing those records on appeal, while Congress and the public continue to demand answers on missing children resulting from family separation.

A police body-worn camera/The St. Thomas Source

On the state and local level, nondisclosure agreements between companies and public officials restrict the public's right to know about policing in their communities. Documents released by Orlando police revealed that Amazon required city officials to sign a nondisclosure agreement to keep details about the Rekognition pilot from public view. The Washington County Sheriff similarly signed an NDA with Amazon, resulting in the withholding of details about facial recognition use.[clxvii] Nondisclosure agreements have become the norm for tech companies, and Amazon claims they are necessary in order to provide free pilots of their services.[clxviii] Such agreements, however, even keep lawmakers in the dark. D.C. police, for example, withheld records from members of Congress on the use of face recognition technology, because their agreements with the company MorphoTrak were stamped "Confidential and Proprietary."[clxix]

The public remains clueless as to how many secrecy agreements exist, and to what extent they hinder information laws across the country. The organization MuckRock found that as of December 2018, the majority of the bids for Amazon's new headquarters were still not available to the public.[clxx] The 20 cities that made Amazon's list of top picks for the HQ2 headquarters were required to sign nondisclosures that required those cities to "give Amazon prior written notice sufficient to allow Amazon to seek a protective order or other remedy," in case a member of the public or reporter filed a public records request.[clxxi] OTG received a response to a request filed with Virginia authorities, showing that the government changed the draft language of their nondisclosure agreement to give Amazon more authority to review Virginia's proposal before releasing it to the public.[clxxii] Many of the nondisclosure agreements are heavily redacted, leaving the public guessing about the incentives that were offered to Amazon. As a result, cities such as New York have introduced legislation to prohibit nondisclosure agreements related to future development projects, arguing that the Amazon's NDA undermined democracy.[clxxiii]

Recommendations

Technology advancements bring important benefits to society, but also can perpetuate dangerous and repressive structures of government. The rapidly increasing use of artificial intelligence and machine learning technologies in national security programs, domestic policing and immigration enforcement merits serious attention.

The AI industry is in dire need of a governing framework that incorporates ethical principles to ensure technology does not fuel systematic human rights violations. Policymakers, together with technologists, civil society groups, academics and companies must address the rampant abuses associated with invasive technologies and the potential dangers posed by government decision-making that relies on machine learning.

As discussed in this report, internal governance structures at most technology companies lack mechanisms to ensure transparency and accountability for invasive surveillance technologies and AI systems. It is imperative, therefore, that policy-makers limit the use of powerful technologies by government, ensuring that safeguards are in place prior adopting any technology.

Lawmakers must increase their oversight role and adopt laws to keep up with the speed of technological advances. Without immediate action, the challenges associated with the application of the new technology becomes more difficult to remedy over time. Currently, companies compete ruthlessly to sell surveillance and AI technologies at the lowest price and win billion-dollar government contracts, fighting for market success at the expense of social responsibility.

Below are recommendations for government entities, companies and the public, that if adopted, will better ensure that new technologies comport with constitutional protections and preserve democratic values.

Congress

Strengthen oversight of private contractors

- Reform the Freedom of Information Act (FOIA) to ensure that government contractors provide the information necessary for the government to respond to FOIA requests relating to surveillance technology and AI systems.

- Reform the Lobbying Disclosure Act to extend requirements to private companies influencing the federal procurement process through direct lobbying, revolving door appointments, or other influences on executive branch policymaking.

- Work with DoD and other agencies to establish transparency requirements for "Other Transaction Agreements" (OTAs).

Establish safeguards for government use of AI technologies

- Require government agencies to establish strict safeguards and privacy standards before purchasing and deploying AI technologies.

- Require DoD and the intelligence agencies to issue regular public reports to Congress (with classified annex) on their use of artificial intelligence and machine learning in counterterrorism and military operations, including testing and evaluation mechanisms used for these technologies.

- Require independent third parties to conduct and publish tests of all AI systems provided to government for predictability and explainability-so that government officials can understand how and why a computer makes the decision it does.

- Create rules and allocate resources to incentivize lawmakers to hire staffers with relevant technical expertise needed for effective oversight over the intelligence community and the military's acquisition of AI systems.[clxxiv]

Combat bias and inaccuracies in law enforcement use of facial recognition services

- Require independent third parties to conduct and publish tests of facial recognition services for accuracy and bias.

- Require law enforcement agencies to establish strict safeguards and privacy standards before purchasing and deploying facial recognition software.

- Mandate transparency from companies regarding the capabilities and limitations of facial recognition technology in terms that customers and consumers can understand.

- Require federal law enforcement agencies that pilot facial recognition to undertake meaningful human review of results prior to making final decisions on whether to adopt the technology. Review should include:

    - Examination of potential violations of human or fundamental rights, personal freedom, or privacy.

    - Examination of risks that the technology could be used to track people based on race, ethnicity, religious or political views.

- Require face recognition use be conditioned on judicial authorization based upon probable cause, to protect against unlawful surveillance and ensure that law enforcement officials only use the technology when there is reasonable suspicion of criminal misconduct.[clxxv]

- Condition federal assistance for facial recognition technology on the public release of internal audits, participation in accuracy testing by the National Institute of Standards and Technology (NIST), and tests for racially biased error rates.

Federal agencies

Improve transparency related to use of AI technologies

- Proactively disclose lists of AI technologies that DoD targets for development, in as much detail as possible without jeopardizing operational security.
- Proactively disclose list of all types of AI technologies the CIA employs or considers, along with policy guidelines to protect privacy and human rights.
- Release the Pentagon's criteria used to evaluate the JEDI contract winner over the first two years (in order to avoid a vendor lock-in scenario).
- Make public the rules governing U.S. use of lethal force outside areas of active hostilities, and whether machine learning or AI may be used in targeting or any other aspect of these military operations.
- Resume releasing, as completely as possible, dates and targeting information for U.S.-led coalition airstrikes in Iraq and Syria, and begin including whether machine learning or AI was used to inform target selection.

Implement oversight and provide accountability for use of AI technologies

- Develop a framework for using facial recognition and other AI that imposes legal obligations on companies selling the technology that sets limits on collection, use, and retention of data, and mandates standards for informed consent, security, accessibility, and accountability.
- Expand ongoing investigations into civil rights infractions to include examining whether surveillance technologies used by police departments have a disparate impact on communities of color.
- Conduct risk assessments before purchasing new facial recognition or AI technologies, as well as privacy impact assessments for programs that will involve U.S. persons data.
- Regulate AI by expanding the powers of sector-specific agencies to oversee, audit, and monitor these technologies by domain.[clxxvi]

State and local legislators

- Require the opportunity for public notice and comment prior to the procurement of facial recognition software and other surveillance tools.
- Require funding for new surveillance technologies be contingent on consultation between communities and law enforcement agencies before acquiring such technologies.
- Consider legislation to prohibit the use of biometric data collection technologies without public consultation and ensure the technologies are not adopted without meaningful oversight mechanisms in place.

Companies

Take measures to mitigate harm of facial recognition services

- Stop the sale of facial recognition technology to government agencies until mechanisms and safeguards are in place to prevent abuse.
- Improve transparency reporting to meet public demand for information on invasive surveillance technology and AI use.

Commit to strengthening, not inhibiting, accountability to the public

- Develop and publicly release AI principles and a policy framework, confirming the following:
    - The company will not pursue technologies whose purpose contravenes widely accepted principles of international law and human rights;
    - The company will not pursue technologies that gather or use information for surveillance violating internationally accepted norms;
    - Neither the company nor its contractors will work with clients who violate international human rights law;
    - The company will consider fully how use of its AI or machine learning technology *could* be weaponized or used to support lethal force, even if the technology is not expressly created for that purpose.
- Commit to transparency and review regarding contracts between the company and government agencies, in the U.S. and beyond. Require a commitment from national security agencies specifying how technologies will be used before government contract is issued.

- Listen and respond to the demands of the employees and shareholders, provide protections for conscientious objectors, employee organizing, and ethical whistleblowers.
- Refrain from implementing nondisclosure agreements or other legal barriers that stand in the way of accountability in the public sector.
- Commit to improving the explainability of AI and machine learning systems to enable oversight and accountability.

Advocates, technology workers, and the public

- Continue to investigate and call attention to companies contracting with military, police, and immigration agencies.
- Defend the rights of employees to declare their values and oppose working with government agencies that engage in human rights abuses and target vulnerable communities.
- Increase public scrutiny on companies that dominate the cloud computing and biometrics data sharing contracts for various federal agencies.
- Conduct more analyses of the campaign contributions made by tech lobbyists to federal legislators and the public policy positions of those lawmakers with regards to cloud computing and other tech contracts.
- Demand more transparency on the influence of tech companies on the federal procurement process, and advocate for stronger oversight of private contractors.

Endnotes

[i] David Streitfeld and Christine Haughney, “Expecting the Unexpected from Jeff Bezos,” New York Times, August 17, 2013, available at: https://www.nytimes.com/2013/08/18/business/expecting-the-unexpected-from-jeff-bezos.html?ref=technology

[ii] Mya Frazier, “Big tech’s bid to control FOIA,” Columbia Journalism Review, February 2, 2018, available at: https://www.cjr.org/business_of_news/facebook-amazon-foia.php

[iii] Martin Austermuhle, “Amazon Insists On Silence From Twenty HQ2 Finalists,” WAMU, January 30, 2018, available at: https://wamu.org/story/18/01/30/amazon-insists-silence-twenty-hq2-finalists/

[iv] Government watchdog group Good Jobs First called the competition a “tax break auction,” and said that Amazon has received more than $2.3 billion in tax breaks and subsidies for its warehouses, data centers, and other facilities since the organization began counting them in 2000.[iv]

[v] Breck Dumas, “Amazon HQ2 facing growing opposition in Northern Virginia following NYC pullout,” The Blaze, February 22, 2019, available at: https://www.theblaze.com/news/amazon-hq2-facing-growing-opposition-in-northern-virginia-following-nyc-pullout

[vi] Ted Mann and Brody Mullins, “As Trump Bashes Amazon, the Government Relies on It,” Wall Street Journal, April 5, 2018, available at: https://www.wsj.com/articles/as-trump-bashes-amazon-the-government-increasingly-relies-on-it-1522920600

[vii] “Innovation Lives Here,” Amazon HQ2 submission, released in redacted form in response to a public records request filed by MuckRock, available at: https://www.muckrock.com/foi/virginia-128/amazon-hq2-bid-finalist-64824/

[viii] Neil Gordon, “Contractors and the True Size of Government,” Project On Government Oversight, October 5, 2017, available at: https://www.pogo.org/analysis/2017/10/contractors-and-true-size-of-government/

[ix] Matthew Yglesias, “Amazon’s $0 corporate income tax bill last year, explained,” Vox, February 20, 2019, available at: https://www.vox.com/2019/2/20/18231742/amazon-federal-taxes-zero-corporate-income

[x] OpenSecrets.org, Center for Responsive Politics, “Annual Lobbying by Amazon.com,” (last visited February 2019) https://www.opensecrets.org/lobby/clientsum.php?id=D000023883&year=2018

[xi] “Cloud Computing for the U.S. Intelligence Community,” Amazon Web Services, available at: https://aws.amazon.com/federal/us-intelligence-community/

[xii] Ted Mann and Brody Mullins, “As Trump Bashes Amazon, the Government Relies on It,” Wall Street Journal, April 5, 2018, available at: https://www.wsj.com/articles/as-trump-bashes-amazon-the-government-increasingly-relies-on-it-1522920600

[xiii] Troy K. Schneider, “CIA CIO: Private cloud 'the best decision we’ve ever made',” FCW, June 14, 2017, available at: https://fcw.com/articles/2017/06/14/cia-cloud-aws.aspx and Naomi Nix, “CIA Tech Official Calls Amazon Cloud Project ‘Transformational’,” Bloomberg, June 20, 2018, available at: https://www.bloomberg.com/news/articles/2018-06-20/cia-tech-official-calls-amazon-cloud-project-transformational

[xiv] Aaron Gregg, “Pentagon doubles down on ‘single-cloud’ strategy for $10 billion contract,” Washington Post, August 5, 2018, available at: https://www.washingtonpost.com/business/capitalbusiness/pentagon-doubles-down-on-single-cloud-strategy-for-10-billion-contract/2018/08/05/352cfee8-972b-11e8-810c-5fa705927d54_story.html

[xv] Lauren C. Williams, "DOD scales back $950M cloud agreement," FCW, March 5, 2018, available at: https://fcw.com/articles/2018/03/05/dod-ream-cloud-contract.aspx

[xvi] "Decision: IBM-U.S. Federal," Government Accountability Office, June 6, 2013, available at: https://www.gao.gov/assets/660/655241.pdf

[xvii] Spencer Soper, Naomi Nix, Ben Brody and Bill Allison, "Amazon's Jeff Bezos Can't Beat Washington, So He's Joining It: The Influence Game," Bloomberg, February 14, 2018, available at: https://www.bloomberg.com/graphics/2018-amazon-lobbying/

[xviii] Ali Breland, "Monopoly critics decry 'Amazon amendment'," The Hill, November 9, 2017, available at: https://thehill.com/policy/cybersecurity/359514-monopoly-critics-decry-amazon-amendment

[xix] For more on ethics requirements for federal appointees, see: Jacob R. Strauss, "Ethics Pledges and Other Executive Branch Appointee Restrictions Since 1993: Historical Perspective, Current Practices, and Options for Change," Congressional Research Service, September 29, 2017, available at: https://fas.org/sgp/crs/misc/R44974.pdf

[xx] Tonya Riley, "Amazon's Bid on a $10 Billion Pentagon Contract Is Riddled With Conflicts of Interest," Mother Jones, December 28, 2018, available at: https://www.motherjones.com/politics/2018/12/amazons-bid-on-a-10-billion-pentagon-contract-is-riddled-with-conflicts-of-interest/

[xxi] Aaron Gregg and Christian Davenport, "Pentagon to review Amazon employee's influence over $10 billion government contract," Washington Post, January 24, 2019, available at: https://www.washingtonpost.com/business/2019/01/24/pentagon-review-amazon-employees-influence-over-billion-government-contract/?utm_term=.67cb349a5fbb

[xxii] Adam Mazmanian, "Judge issues stay in JEDI protest case," FCW, February 19, 2019, available at: https://fcw.com/articles/2019/02/19/oracle-jedi-lawsuit-stay.aspx

[xxiii] Naomi Nix, "Inside the Nasty Battle to Stop Amazon From Winning the Pentagon's Cloud Contract," Bloomberg, December 20, 2018, available at: https://www.bloomberg.com/news/features/2018-12-20/tech-giants-fight-over-10-billion-pentagon-cloud-contract

[xxiv] For more on the Pentagon revolving door, see: Mandy Smithberger, "Brass Parachutes: The Problem of the Pentagon Revolving Door," Project On Government Oversight, November 5, 2018, available at: https://www.pogo.org/report/2018/11/brass-parachutes/

[xxv] Paris Martineau, "Lawmakers Seek Review of Pentagon Contract Thought to Favor Amazon," Wired, October 25, 2018, available at: https://www.wired.com/story/lawmakers-seek-review-pentagon-contract-thought-favor-amazon/

[xxvi] Jason Miller, "FBI, DoD IG conducting preliminary investigation into JEDI, procurements," Federal News Network, March 4, 2019, available at: https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/03/fbi-dod-ig-conducting-preliminary-investigation-into-jedi-procurements/

[xxvii] "DoD cloud strategy," December 2018, available at: https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF

[xxviii] Id. 5.

[xxix] Frank Konkel, "FBI's Counterterrorism Investigations Now Run on Amazon," Nextgov, November 29, 2018, available at: https://www.nextgov.com/it-modernization/2018/11/fbis-counterterrorism-investigations-now-run-amazon/153133/

[xxx] Michael C. Horowitz, "The Algorithms of August," Foreign Policy, September 12, 2018, available at: https://foreignpolicy.com/2018/09/12/will-the-united-states-lose-the-artificial-intelligence-arms-race/

[xxxi] "Executive Order on Maintaining American Leadership in Artificial Intelligence," The White House, February 11, 2019, available at: https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

[xxxii] "Summary of the Department of Defense Artificial Intelligence Strategy," Department of Defense, February 12, 2019, available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[xxxiii] "Department of Defense Directive Number 3000.09," November 21, 2012, available at: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

[xxxiv] Semi-autonomous weapons can sense the environment and make decisions on their own, but require a human to act. Autonomous weapons can sense, decide, and act without any human intervention. See: Paul Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Company, 2018, pg. 29-30

[xxxv] Paul Scharre, , Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Company, 2018, pg. 49

[xxxvi] Nafeez Ahmed, "Pentagon Wants to Predict Anti-Trump Protests Using Social Media Surveillance," VICE, October 30, 2018, available at: https://motherboard.vice.com/en_us/article/7x3g4x/pentagon-wants-to-predict-anti-trump-protests-using-social-media-surveillance

[xxxvii] For more on the potential military uses of AI, see: "AI and the Military: Forever Altering Strategic Stability", T4GS Reports, February 13, 2019, available at: http://www.tech4gs.org/ai-and-human- decision-making.html

[xxxviii] Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," U.S. Department of Defense, July 21, 2017, available at: https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/

[xxxix] Kate Conger, "Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program," Gizmodo, June 1, 2018, available at: https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620

[xl] Amanda Ziadeh, "CIA Finds Security, AI Opportunities in Cloud," GovernmentCIO, June 20, 2018, available at: https://www.governmentciomedia.com/cia-finds-security-ai-opportunities-cloud

[xli] Nicole Nguyen, "Amazon Bought A Router Company You've Never Heard Of. Here Is Why It's A Huge Deal." Buzzfeed, February 12, 2019, available at: https://www.buzzfeednews.com/article/nicolenguyen/amazon-acquisition-eero-routers-privacy

[xlii] Zack Whittaker, "Amazon won't say if it hands your Echo data to the government," Zero Day, January 16, 2018, available at: https://www.zdnet.com/article/amazon-the-least-transparent-tech-company/

[xliii] "Artificial Intelligence at Google: Our Principles," Google, available at: https://ai.google/principles/

[xliv] Lee Fang, "Google Hired Gig Economy Workers to Improve Artificial Intelligence in Controversial Drone-Targeting Project," The Intercept, February 4, 2019, available at: https://theintercept.com/2019/02/04/google-ai-project-maven-figure-eight/

[xlv] Sheera Frenkel, "Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration," New York Times, June 19, 2018, available at: https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html

[xlvi] Lee Fang, "Amazon Promises "Unwavering" Commitment to Police, Military Clients Using AI Technology," The Intercept, July 30, 2018, available at: https://theintercept.com/2018/07/30/amazon-facial-recognition-police-military/

[xlvii] David Sanger, "Microsoft Says It Will Sell Pentagon Artificial Intelligence and Other Advanced Technology," New York Times, October 26, 2018, available at: https://www.nytimes.com/2018/10/26/us/politics/ai-microsoft-pentagon.html

[xlviii] Lucas Matney, "Group of employees calls for end to Microsoft's $480M HoloLens military contract," TechCrunch, February 23, 2019, available at: https://techcrunch.com/2019/02/23/group-of-employees-call-for-end-to-microsofts-480m-hololens-military-contract/

[xlix] Kevin Roose, "Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts," New York Times, March 4, 2019, available at: https://www.nytimes.com/2019/03/04/technology/technology-military-contracts.html

[l] "Summary of the Department of Defense Artificial Intelligence Strategy," Department of Defense, February 12, 2019, available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[li] Kelley M. Sayler and Daniel S. Hoadley, "Artificial Intelligence and National Security," Congressional Research Service, January 30, 2019, available at: https://fas.org/sgp/crs/natsec/R45178.pdf

[lii] "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD," JASON, The MITRE Corporation, January 2017, available at: https://fas.org/irp/agency/dod/jason/ai-dod.pdf

[liii] Sayler and Hoadley, pg. 6-7

[liv] Paul Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Company, 2018, pg. 187

[lv] Sayler and Hoadley, pg. 31

[lvi] Id. pg. 182-183.

[lvii] Tom Simonite, "Startup Working on Contentious Pentagon AI Project was Hacked," Wired, June 12, 2018, available at: https://www.wired.com/story/startup-working-on-contentious-pentagon-ai-project-was-hacked/

[lviii] "AI and the Military: Forever Altering Strategic Stability", T4GS Reports, February 13, 2019, pg. 9-10 available at: http://www.tech4gs.org/ai-and-human- decision-making.html

[lix] "Recommendations," Defense Innovation Board, available at: https://innovation.defense.gov/Recommendations/

[lx] Jenna McLaughlin and Zach Dorfman, "At the CIA, a fix to communications system that left trail of dead agents remains elusive," Yahoo News, December 6, 2018, available at: https://news.yahoo.com/cia-fix-communications-system-left-trail-dead-agents-remains-elusive-100046908.html

[lxi] Tom Simonite, "Startup Working on Contentious Pentagon AI Project was Hacked," Wired, June 12, 2018, available at: https://www.wired.com/story/startup-working-on-contentious-pentagon-ai-project-was-hacked/

[lxii] Adam Mazmanian, "OTA comes under increased scrutiny," Defense Systems, June 14, 2018, available at: https://defensesystems.com/articles/2018/06/15/congress-ota.aspx

[lxiii] Darwin McDaniel, "Microsoft Wins $480M Army Augmented Reality Tech Prototyping OTA," GovCon Wire, November 29, 2018, available at: https://www.govconwire.com/2018/11/microsoft-wins-480m-army-augmented-reality-tech-prototyping-ota/

[lxiv] "Protecting her own image" - Gina Haspel nomination process shows need for classification reform," Open the Government, May 17, 2018, available at: https://www.openthegovernment.org/2018/05/17/protecting-her-own-image-gina-haspel-nomination-process-shows-need-for-classification-reform-2/

[lxv] Alex Hopkins, “Airwars annual assessment 2018: despite significant falls in casualty numbers, Syria’s civilians remained at high risk,” Airwars, January 2019, available at: https://airwars.org/report/airwars-annual-assessment-2018/

[lxvi] Trevor Aaronson, “Defense Department Abruptly Stopped Releasing Key Details On Strikes in War Against ISIS,” The Intercept, January 9, 2019, available at: https://theintercept.com/2019/01/09/syria-isis-airstrikes-us-military/

[lxvii] Patrick Tucker, “Project Maven Overseer Will Lead Pentagon’s New AI Center,” Defense One, December 14, 2018, available at: https://www.defenseone.com/technology/2018/12/project-maven-overseer-will-lead-pentagons-new-ai-center/153555/

[lxviii] Dan de Luce and Paul Cleary, “Obama’s Most Dangerous Drone Tactic is Here to Stay,” Foreign Policy, April 5, 2016, available at: https://foreignpolicy.com/2016/04/05/obamas-most-dangerous-drone-tactic-is-here-to-stay/

[lxix] Stephen Tankel, “Donald Trump’s Shadow War,” Politico, May 9, 2018, available at: https://www.politico.com/magazine/story/2018/05/09/donald-trumps-shadow-war-218327

[lxx] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, “Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2,” IEEE, 2017, available at: http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html

[lxxi] An Amazon Employee, “Why My Company Shouldn’t Sell Facial Recognition Technology Tech to Police,” Medium, October 16, 2018, available at: https://medium.com/s/powertrip/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac

[lxxii] Ranju Das, “Amazon Rekognition Announces Real-Time Face Recognition, Support for Recognition of Text in Image, and Improved Face Detection,” AWS Machine Learning Blog, November 21, 2017, available at: https://aws.amazon.com/blogs/machine-learning/amazon-rekognition-announces-real-time-face-recognition-support-for-recognition-of-text-in-image-and-improved-face-detection/

[lxxiii] An Amazon Employee, “Why My Company Shouldn’t Sell Facial Recognition Technology Tech to Police,” Medium, October 16, 2018, available at: https://medium.com/s/powertrip/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac

[lxxiv] Matt Cagle & Nicole Ozer, “Amazon teams up with government to deploy dangerous New Racial Recognition Technology,” ACLU, May 22, 2018, available at: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new

[lxxv] “Risks of Sales of Facial Recognition Software,” Amazon.com, Inc., 2019, available at: https://static1.squarespace.com/static/57693891579fb3ab7149f04b/t/5c2cf4f86d2a73e6a9cfd391/1546450246520/Amazon+Prohibit+Sales+Resolution ; Matt McFarland, “Amazon shareholders call for halt of facial recognition sales to police,” CNN, June 18, 2018, available at: https://money.cnn.com/2018/06/18/technology/amazon-facial-recognition/index.html

[lxxvi] Georgetown Law Center on Privacy & Technology, “The Perpetual Lineup,” October 2016, available at: https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf

[lxxvii] Sidney Fussell, “Chicago Advances Bill Allowing Police Drones to Surveil Protesters,” Gizmodo, May 3, 2018, available at: https://gizmodo.com/chicago-advances-bill-allowing-police-drones-to-surveil-1825749338

[lxxviii] “You are not alone,” Fight for the Future, Whistleblower resources, available at: https://www.speakout.tech/

[lxxix] "Risks of Sales of Facial Recognition Software," Amazon.com, Inc. Shareholders, 2019, available at: https://static1.squarespace.com/static/57693891579fb3ab7149f04b/t/5c2cf4f86d2a73e6a9cfd391/1546450246520/Amazon+Prohibit+Sales+Resolution

[lxxx] Spencer Ackerman & Betsy Woodruff, "Defense Contractors Cashing In On Immigrant Kids' Detention," Daily Beast, June 14, 2018, available at: https://www.thedailybeast.com/defense-contractors-cashing-in-on-immigrant-kids-detention; Aura Bogado, Ziva Branstetter, and Vanessa Swales, "Defense contractor detained migrant kids in vacant Phoenix office building," Reveal, July 6, 2018, available at: https://www.revealnews.org/article/defense-contractor-detained-migrant-kids-in-vacant-phoenix-office-building/

[lxxxi] Kate Conger, "Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts With Law Enforcement," Gizmodo, June 21, 2018, available at; https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509.

[lxxxii] Jacob Kastrenakes, "Salesforce employees ask CEO to 're-examine' contract with border protection agency," The Verge, June 25, 2018, available at: https://www.theverge.com/2018/6/25/17504154/salesforce-employee-letter-border-protection-ice-immigration-cbp

[lxxxiii] Sheera Frenkel, "Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration," New York Times, June 19, 2018, available at: https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html; Tom Keane, "Federal agencies continue to advance capabilities with Azure Government," Microsoft, January 24, 2018, available at: https://blogs.msdn.microsoft.com/azuregov/2018/01/24/federal-agencies-continue-to-advance-capabilities-with-azure-government/

[lxxxiv] Letter from Microsoft employees to CEO Satya Nadella, available at: https://int.nyt.com/data/documenthelper/46-microsoft-employee-letter-ice/323507fcbddb9d0c59ff/optimized/full.pdf#page=1

[lxxxv] Kate Conger, "Microsoft CEO Downplays ICE Contract in Email to Employees," Gizmodo, June 20, 2018, available at: https://gizmodo.com/microsoft-ceo-downplays-ice-contract-in-email-to-employ-1826973750

[lxxxvi] Tom Keane, "Federal agencies continue to advance capabilities with Azure Government," Microsoft, January 24, 2018, available at: https://blogs.msdn.microsoft.com/azuregov/2018/01/24/federal-agencies-continue-to-advance-capabilities-with-azure-government/

[lxxxvii] Open the Government, Closing Democracy's Window, VI. The Department of Homeland Security, March 2018: available at: https://www.openthegovernment.org/wp-content/uploads/other-files/CDW%20FINAL.pdf

[lxxxviii] See "ICE is Making its Massive Data Collection Effort Secret as it Labels More and More Immigrants 'Gang Members,'" The Appeal, October 3, 2017, available at: https://theappeal.org/ice-is-making-its-massive-data-collection-effort-secret-as-it-labels-more-and-more-immigrants-gang-d324f2889b6/

[lxxxix] "Who is Behind ICE? The Tech and Data Companies Fueling Deportations," The National Immigration Project of the National Lawyers Guild, Immigration Defense Project & Mijente, October 2018, available at: https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf

[xc] Id.

[xci] Id.; see also Department of Homeland Security, Privacy Impact Assessment, "United States - Mexico Entry/Exit Data Sharing Initiative," December 14, 2017, available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-usmexicoentryexitdatasharinginitiative-december2017.pdf

[xcii] William Alden, “Palantir’s relationship with America’s spies has been worse than you’d think,” BuzzFeed News, April 21, 2017, available at: https://www.cnbc.com/2017/04/21/buzzfeed-palantir-loses-relationship-with-nsa-ceo-karp-bashes-trump.html

[xciii] Matt Burns, “Leaked Palantir Doc Reveals Uses, Specific Functions And Key Clients,” Tech Crunch, January 11, 2015, available at: https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/

[xciv] Center for Responsive Politics, OpenSecrets, Palantir Technologies, available at (last visited Feb. 2019): https://www.opensecrets.org/revolving/search_result.php?priv=Palantir+Technologies; Justin Elliot, “Meet the Hundreds of Officials Trump Has Quietly Installed Across the Government,” ProPublica, March 8, 2017, available at: https://www.propublica.org/article/meet-hundreds-of-officials-trump-has-quietly-installed-across-government

[xcv] Mark Harris, “How Peter Thiel’s Secretive Data Company Pushed into Policing,” Wired, August 8, 2017, available at: https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/

[xcvi] Spencer Woodman, “Palantir Provides the Engine for Donald Trump’s Deportation Machine,” The Intercept, March 2, 2018, available at: https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/

[xcvii] AWS was one of the first cloud service providers to meet the Federal Risk and Authorization Management Program (FedRAMP) Hight baseline, giving the government the ability to leverage AWS Cloud for contracts that manage highly sensitive data. See “Amazon Web Services Achieves FedRAMP High Authorization,” AWS Government, Education, & Nonprofits blog, June 23, 2016, available at: https://aws.amazon.com/blogs/publicsector/amazon-web-services-achieves-fedramp-high-authorization/

[xcviii] Karen Hao, “Amazon is the invisible backbone behind ICE’s immigration crackdown,” MIT Technology Review, October 22, 2018, available at: https://www.technologyreview.com/s/612335/amazon-is-the-invisible-backbone-behind-ices-immigration-crackdown/; see Federal Risk and Authorization Management Program (FedRAMP), available at: https://marketplace.fedramp.gov/#/products?sort=-authorizations (last visited February 27, 2019).

[xcix] An Amazon Employee, “Why My Company Shouldn’t Sell Facial Recognition Technology Tech to Police,” Medium, October 16, 2018, available at: https://medium.com/s/powertrip/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac; Peter Waldman, Lizette Chapman, and Jordan Robertson, “Palantir Knows Everything About You, Bloomberg Businessweek, April 19, 2018, available at: https://www.bloomberg.com/features/2018-palantir-peter-thiel/

[c] Joan Friedland, “How ICE Uses Databases and Information-Sharing to Deport Immigrants, National Immigration Law Center, January 25, 2019, available at: https://www.nilc.org/2018/01/25/how-ice-uses-databases-and-information-sharing-to-deport-immigrants/

[ci] “Understanding Allegations of Gang Membership/Affiliation in Immigration Cases,” Immigrant Legal Resource Center, April 2017, available at: https://www.ilrc.org/sites/default/files/resources/ilrc_gang_advisory-20170509.pdf

[cii] Thomas Nolan, “The Trouble with So-Called ‘Gang Databases’: No Refuge in the ‘Sanctuary,’” American Constitution Society, June 27, 2018, available at: https://www.acslaw.org/acsblog/the-trouble-with-so-called-gang-databases-no-refuge-in-the-sanctuary/

[ciii] David Bier, “U.S. Citizens Targeted by ICE: U.S. Citizens Targeted by Immigration and Customs Enforcement in Texas,” Cato Institute, August 29, 2018, https://www.cato.org/publications/immigration-research-policy-brief/us-citizens-targeted-ice-us-citizens-targeted

[civ] Joel Rubin & Paige St. John, “How a U.S. citizen was mistakenly targeted for deportation. He’s not alone,” LA Times, November 29, 2017, available at: https://www.latimes.com/local/lanow/la-me-ice-citizen-arrest-20171129-story.html

[cv] "Who is Behind ICE? The Tech and Data Companies Fueling Deportations," The National Immigration Project of the National Lawyers Guild, Immigration Defense Project & Mijente, October 2018, available at: https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf

[cvi] OpenSecrets.org, Center for Responsive Politics, "Annual Lobbying by Amazon.com," (last visited Feburary 2019) available at: https://www.opensecrets.org/lobby/clientsum.php?id=D000023883&year=2018

[cvii] Davey Alba & Caroline O'Donovan, "Amazon Won't Say It Doesn't Work With ICE," BuzzFeed, December 12, 2018, available at: https://www.buzzfeednews.com/article/daveyalba/amazon-wont-say-it-doesnt-work-with-ice

[cviii] Andrea Peterson & Jake Laperruque, "Amazon Pushes ICE to Buy Its Face Recognition Surveillance Tech," Project on Government Oversight, October 24, 2018, available at: https://www.pogo.org/investigation/2018/10/amazon-pushes-ice-to-buy-its-face-recognition-surveillance-tech/

[cix] Matt Cagle & Nicole Ozer, "Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology, ACLU, May 22, 2018, available at: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new.

[cx] Amazon Rekognition FAQ's, Video Analytics, available at (last visited February 27, 2019): https://aws.amazon.com/rekognition/faqs/?ascsubtag=f1c3d105da9c6a53eb9dcdf301c58a280adb5e40&tag=gizmodoamzn-20#Video_Analytics

[cxi] Phillip Jackson, "Federal judge rules Memphis police violated consent decree after spying on protesters," Memphis Commercial Appeal (USA Today Network), October 26, 2018, available at: https://www.commercialappeal.com/story/news/2018/10/26/memphis-police-violated-decree-spying-protesters/1780238002/; Ali Winston, "Did the Police Spy on Black Lives Matter Protesters? The Answer May Soon Come Out," The New York Times, January 14, 2018, available at: https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html

[cxii] Open the Government, Closing Democracy's Window, V. The Department of Justice, March 2018: available at: https://www.openthegovernment.org/wp-content/uploads/other-files/CDW%20FINAL.pdf

[cxiii] Jake Laperruque, "Facing the Future of Surveillance," The Constitution Project's Task Force on Facial Recognition Surveillance, Project On Government Oversight, March 4, 2019, available at: https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/

[cxiv] Matt Cagle & Nicole A. Ozer, "Amazon Teams up with Law Enforcement to Deploy Dangerous New Face Recognition Technology. Here's How it's used in Washington Country," ACLU, May 22, 2018, available at: https://aclu-or.org/en/news/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology-heres-how-its

[cxv] Id.

[cxvi] Elizabeth Dwoskin, "Amazon is selling facial recognition to law enforcement — for a fistful of dollars," May 22, 2018, available at: https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/?utm_term=.a588f61c9b10

[cxvii] Dan Robitzski, "Cops Are Using Amazon's Facial Recognition Software Wrong," Futurism, February 1, 2019, available at: https://futurism.com/cops-amazon-facial-recognition

[cxviii] "Florida Letter to Orlando City Council, Re: Amazon Rekognition" ACLU of Florida, January 25, 2018, available at: https://www.aclufl.org/sites/default/files/aclu_of_florida_letter_to_orlando_city_council_re_amazon_rekognition.pdf

[cxix] Sidney Fussell, “Amazon and Orlando Cops’ Controversial Face Recognition Pilot Isn’t Over,” Gizmodo, July 10, 2018, available at: https://gizmodo.com/amazon-and-orlando-cops-controversial-face-recognition-1827483145
[cxx] Davey Alba, “Here's How Orlando Is Using Amazon's Facial Recognition Technology,” BuzzFeed, October 30, 2018, available at: https://www.buzzfeednews.com/article/daveyalba/amazon-facial-recognition-orlando-police-department

[cxxi] Jon Penney, “Chilling Effects: Online Surveillance and Wikipedia Use,” Berkeley Technology Law Journal, April 27, 2016, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

[cxxii] Georgetown Law Center on Privacy & Technology, “The Perpetual Lineup,” October 2016, available at: https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf
[cxxiii] Joseph and Lipp, “IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color,” available at https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/

[cxxiv] “Law Enforcement Use of Facial Recognition Technology,” Hearing before the Committee on Oversight and Government Reform, March 22, 2017, available at: https://docs.house.gov/meetings/GO/GO00/20170322/105757/HHRG-115-GO00-Transcript-20170322.pdf. See also MuckRock, Response to FOIA request No. 2018-FOIA-04133, June 27, 2018, available at https://www.muckrock.com/foi/washington-48/facial-recognition-systems-metropolitan-police-department-35563/

[cxxv] Jennifer Lynch, “Face Off: Law Enforcement Use of Face Recognition Technology,” Electronic Frontier Foundation, February 12, 2018, available at: https://www.eff.org/wp/law-enforcement-use-face-recognition

[cxxvi] Id; & Jesse Franzblau, “FBI’s Limited Restrictions on Biometrics Data Sharing Raises Secrecy and Privacy Concerns,” Open the Government, August 7, 2017, available at: https://www.openthegovernment.org/2017/08/07/fbis-limited-restrictions-on-biometrics-data-sharing-raises-secrecy-and-privacy-concerns/

[cxxvii] Trevor Timm, “‘Shock, Anger, Disappointment’: An Amazon Employee Speaks Out,” Medium, October 16, 2018, available at: https://medium.com/s/oversight/88d927792950

[cxxviii] Larry Hardesty, ‘Study finds gender and skin-type bias in commercial artificial-intelligence systems,” MIT News Office, February 11, 2018, available at: http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

[cxxix] “AI, Ain’t I a Woman?” Joy Boulamwini, January 28, 2018, available at: https://www.youtube.com/watch?v=QxuyfWoVV98

[cxxx] Joy Boulamwini, “When the Robot Doesn’t See Dark Skin,” New York Times, June 21, 2018, available at: https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html

[cxxxi] Brad Smith, “Face recognition: It’s time for action,” Microsoft, December 6, 2018, available at: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

[cxxxii] See Criminal Justice Fact Sheet, NAACP (2009), available at: http://www.naacp.org/criminal-justice-fact-sheet.

[cxxxiii] Deborah Raji & Joy Boulamwini, “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,” available at: http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf.

[cxxxiv] Natasha Singer, “Amazon Is Pushing Facial Technology That a Study Says Could Be Biased, New York Times, January 24, 2019, available at: https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

[cxxxv] "ACLU Comment on Google's Commitment not to Sell a Facial Recognition Surveillance Product," ACLU, December 13, 2018, available at: https://www.aclu.org/news/aclu-comment-googles-commitment-not-sell-facial-recognition-surveillance-product.

[cxxxvi] Rich Sauer, "Six principles to guide Microsoft's facial recognition work," Microsoft, December 17, 2018, available at: https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/

[cxxxvii] Matt Wood, "Thoughts on Recent Research Paper and Associated Article on Amazon Rekognition," Amazon Machine Learning Blog, January 26, 2019, available at: https://aws.amazon.com/blogs/machine-learning/thoughts-on-recent-research-paper-and-associated-article-on-amazon-rekognition/; "Amazon defends Rekognition from MIT findings, which it says is outdated," CIO Bulletin, February 4, 2019, available at: http://www.ciobulletin.com/software/mit-opposes-amazon-selling-recognition

[cxxxviii] Zoe Kleinman, "Amazon: Facial recognition bias claims are 'misleading'," BBC News, February 4, 2019, available at: https://www.bbc.com/news/technology-47117299

[cxxxix] Evan Selinger, "Amazon Needs to Stop Providing Facial Recognition Tech for the Government," Meduim, June 21, 2018, available at: https://medium.com/s/story/amazon-needs-to-stop-providing-facial-recognition-tech-for-the-government-795741a016a6

[cxl] Meredith Whittaker, Kate Crawford, Roel Dobbe, Genevieve Fried, Elizabeth Kaziunas, Varoon Mathur, Sarah Myers West, Rashida Richardson, Jason Schultz, Oscar Schwarz, "AI Now Report 2018," The AI Now Institute, December 2018, available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf

[cxli] Id.

[cxlii] India McKinney, "A Surveillance Wall Is Not a Good Alternative to a Concrete Wall," Electronic Frontier Foundation, January 29, 2019, available at: https://www.eff.org/deeplinks/2019/01/surveillance-wall-not-good-alternative-concrete-wall

[cxliii] "CBC Expresses Privacy, Racial Bias Concerns about Facial Recognition Technology Marketed, Sold by Amazon," Congressional Black Caucus, Press Release, May 24, 2018, available at: https://cbc.house.gov/news/documentsingle.aspx?DocumentID=898

[cxliv] Natasha Singer, "Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says," New York Times, July 26, 2018, available at: https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html?partner=rss&emc=rss

[cxlv] Sidney Fussell, "Can We Make Non-Racist Face Recognition?" Gizmodo, July 25, 2018, available at: https://gizmodo.com/can-we-make-non-racist-face-recognition-1827639249

[cxlvi] Letter from Senator Ed Markey (D-MA), Rep. Luis Gutierrez (D-IL) and Rep. Mark DeSaulnier (D-CA) to Jeff Bezos, July 26, 2018, available at https://www.markey.senate.gov/imo/media/doc/Amazon%20Facial%20Recognition%20Tech.pdf

[cxlvii] Id.

[cxlviii] Letter from Members of Congress to Jeff Bezos, July 27, 2018, available at: https://gomez.house.gov/uploadedfiles/07272018_amazon_rekognition_letter_final.pdf

[cxlix] Letter from Senators to the Comptroller General of the United States, July 31, 2018, available at: https://www.wyden.senate.gov/imo/media/doc/073118%20GAO%20Facial%20Recognition%20Request%20(as%20submitted).pdf

[cl] Letter from Members of Congress to Jeff Bezos, November 29, 2018, available at: https://www.markey.senate.gov/imo/media/doc/Bicameral%20Amazon%20Recognition.pdf

[cli] Bryan Menagus, "U.S. Congressman Wants to Make Amazon Testify on its Facial Recognition Tool," Gizmodo, February 12, 2019, available at: https://gizmodo.com/u-s-congressman-wants-to-make-amazon-testify-on-its-fa-1832565669

[clii] Davey Alba & Lissandra Villa, "As Concerns Over Facial Recognition Grow, Members Of Congress Are Considering Their Next Move," BuzzFeed news, February 20, 2019, available at: https://www.buzzfeednews.com/article/daveyalba/house-oversight-committee-hearing-facial-recognition

[cliii] Brad Smith, "Face recognition: It's time for action," Microsoft, December 6, 2018, available at: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

[cliv] Keumars Afifi-Sabet, "Amazon outlines regulatory framework for facial recognition," ITPro, February 8, 2019, available at: https://www.itpro.co.uk/technology/32952/amazon-outlines-regulatory-framework-for-facial-recognition; Matt Wood, "Thoughts on Recent Research Paper and Associated Article on Amazon Rekognition," Amazon Machine Learning Blog, January 26, 2019, available at: https://aws.amazon.com/blogs/machine-learning/thoughts-on-recent-research-paper-and-associated-article-on-amazon-rekognition/

[clv] Keumars Afifi-Sabet, "Amazon outlines regulatory framework for facial recognition," ITPRO, February 8, 2019, available at: https://www.itpro.co.uk/technology/32952/amazon-outlines-regulatory-framework-for-facial-recognition;

[clvi] San Francisco Proposal, Acquisition of Surveillance Technology, January 2019, available at: https://cdn.vox-cdn.com/uploads/chorus_asset/file/13723917/ORD__Acquisition_of_Surveillance_Technology.pdf

[clvii] Colin Lecher, "San Francisco proposal would ban government facial recognition use in the city," The Verge, January 29, 2019, available at: https://www.theverge.com/2019/1/29/18202602/san-francisco-facial-recognition-ban-proposal

[clviii] "At Act Establishing a Moratorium on Face Recognition and other Remote Biometric Surveillance Systems," Massachusetts Legislature, February 2019, available at: https://malegislature.gov/Bills/191/SD671

[clix] "Concerning the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology," Washington State Legislature, February 2019, available at: https://app.leg.wa.gov/billsummary?BillNumber=5528&Year=2019&Initiative=false

[clx] Community Control over Police Surveillance," ACLU, available at (last visited February 28, 2019): https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance

[clxi] CIA response letter, FOIA request F-2014-00355, March 27, 2014

[clxii] NSA response letter, FOIA case 76886A, August 17, 2016

[clxiii] "EPIC FOIA: EPIC Seeks Details of ICE, Palantir Deal," Electronic Privacy Information Center, August 15, 2017, available at: https://epic.org/2017/08/epic-foia-epic-seeks-details-o.html

[clxiv] Beryl Lipton, "ACLU leads coalition urging limits on use of facial recognition," MuckRock, January 17, 2019, available at: https://www.muckrock.com/news/archives/2019/jan/17/ACLU-facial-recognition/

[clxv] ICE response letters to Open the Government

[clxvi] Jesse Franzblau, "Newly released memo reveals secretary of homeland security signed off on family separation policy," Open the Government, September 24, 2018, available at:

https://www.openthegovernment.org/2018/09/24/newly-released-memo-reveals-secretary-of-homeland-security-signed-off-on-family-separation-policy/; U.S. Department of Health and Human Services, Office of the Inspector General, Separated Children Placed in Office of Refugee Resettlement Care, January 2019, available at: https://oig.hhs.gov/oei/reports/oei-BL-18-00511.pdf

[clxvii] ACLU public records requests to Orland Police Department related to Amazon Rekognition facial recognition service, ACLU, January 18, 2018, available at: https://www.aclunc.org/docs/20180522_ARD.pdf#page=7

[clxviii] Evan Selinger, "Amazon Needs to Stop Providing Facial Recognition Tech for the Government," Meduim, June 21, 2018, available at: https://medium.com/s/story/amazon-needs-to-stop-providing-facial-recognition-tech-for-the-government-795741a016a6

[clxix] Letter from the DC Office of the Attorney General, to the U.S. House Committee on Oversight and Government Reform, June 7, 2017.

[clxx] Paxtyn Merten, "#AmazonHQ2 and transparency: An ongoing post-mortem," MuckRock, December 7, 2018, available at: https://www.muckrock.com/news/archives/2018/dec/07/amazon-hq-post-mortem/

[clxxi] Zoe Rosenberg, "City Council seeks to bar Amazon-style NDAs in future development deals," NY Curbed, December 20, 2018, available at: https://ny.curbed.com/2018/12/20/18150100/amazon-hq2-nda-new-york-city-council

[clxxii] Virginia public records response, obtained by Open the Government, February 11, 2019 (in author files).

[clxxiii] Zoe Rosenberg, "City Council seeks to bar Amazon-style NDAs in future development deals," NY Curbed, December 20, 2018, available at: https://ny.curbed.com/2018/12/20/18150100/amazon-hq2-nda-new-york-city-council

[clxxiv] For further information on increasing Congressional oversight capacity, see: "Strengthening Congressional Oversight of the Intelligence Community," R Street, Demand Progress, FreedomWorks, and EFF, September 2016, https://s3.amazonaws.com/demandprogress/reports/Strengthening_Congressional_Oversight_of_the_IC_White_Paper_Sept_2016.pdf

[clxxv] The Constitution Project's Task Force on Facial Recognition Surveillance has published detailed recommendations to guide policymakers in considering how to regulate facial recognition surveillance in a manner that both protects constitutional principles and aids public safety. See Jake Laperruque, "Facing the Future of Surveillance," The Constitution Project's Task Force on Facial Recognition Surveillance, Project On Government Oversight, March 4, 2019, available at: https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/

[clxxvi] Experts recommend that sectors such as health, education, criminal justice and public welfare, all have their own regulatory frameworks that take into account nuances and sectoral expertise of each issue area. Examples of sector-specific approaches include the U.S. Federal Aviation Administration and the National Highway Traffic Safety Administration. See AI Now Report 2018, December 2018, available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf.