The Global Expansion of AI Surveillance

Steven Feldstein

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

+ CONTENTS

Executive Summary

Artificial intelligence (AI) technology is rapidly proliferating around the world. Startling developments keep emerging, from the onset of deepfake videos that blur the line between truth and falsehood, to advanced algorithms that can beat the best players in the world in multiplayer poker. Businesses harness AI capabilities to improve analytic processing; city officials tap AI to monitor traffic congestion and oversee smart energy metering. Yet a growing number of states are deploying advanced AI surveillance tools to monitor, track, and surveil citizens to accomplish a range of policy objectives—some lawful, others that violate human rights, and many of which fall into a murky middle ground.

In order to appropriately address the effects of this technology, it is important to first understand where these tools are being deployed and how they are being used. Unfortunately, such information is scarce. To provide greater clarity, this paper presents an AI Global Surveillance (AIGS) Index—representing one of the first research efforts of its kind. The index compiles empirical data on AI surveillance use for 176 countries around the world. It does not distinguish between legitimate and unlawful uses of AI surveillance. Rather, the purpose of the research is to show how new surveillance capabilities are transforming the ability of governments to monitor and track individuals or systems. It specifically asks:

- Which countries are adopting AI surveillance technology?
- What specific types of AI surveillance are governments deploying?
- Which countries and companies are supplying this technology?

Key Findings:

- AI surveillance technology is spreading at a faster rate to a wider range of countries than experts have commonly understood. At least seventy-five out of 176 countries globally are actively using AI technologies for surveillance purposes. This includes: smart city/safe city platforms (fifty-six countries), facial recognition systems (sixty-four countries), and smart policing (fifty-two countries).

- China is a major driver of AI surveillance worldwide. Technology linked to Chinese companies—particularly Huawei, Hikvision, Dahua, and ZTE—supply AI surveillance technology in sixty-three countries, thirty-six of which have signed onto China's Belt and Road Initiative (BRI). Huawei alone is responsible for providing AI surveillance technology to at least fifty countries worldwide. No other company comes close. The next largest non-Chinese supplier of AI surveillance tech is Japan's NEC Corporation (fourteen countries).

- Chinese product pitches are often accompanied by soft loans to encourage governments to purchase their equipment. These tactics are particularly relevant in countries like Kenya, Laos, Mongolia, Uganda, and Uzbekistan—which otherwise might not access this technology. This raises troubling questions about the extent to which the Chinese government is subsidizing the purchase of advanced repressive technology.

- But China is not the only country supplying advanced surveillance tech worldwide. U.S. companies are also active in this space. AI surveillance technology supplied by U.S. firms is present in thirty-two countries. The most significant U.S. companies are IBM (eleven countries), Palantir (nine countries), and Cisco (six countries). Other companies based in liberal democracies—France, Germany, Israel, Japan—are also playing important roles in proliferating this technology. Democracies are not taking adequate steps to monitor and control the spread of sophisticated technologies linked to a range of violations.

- Liberal democracies are major users of AI surveillance. The index shows that 51 percent of advanced democracies deploy AI surveillance systems. In contrast, 37 percent of closed autocratic states, 41 percent of electoral autocratic/competitive autocratic states, and 41 percent of electoral democracies/illiberal democracies deploy AI surveillance technology.[1] Governments in full democracies are deploying a range of surveillance technology, from safe city platforms to facial recognition cameras. This does not inevitably mean that democracies are abusing these systems. The most important factor determining whether governments will deploy this technology for repressive purposes is the quality of their governance.

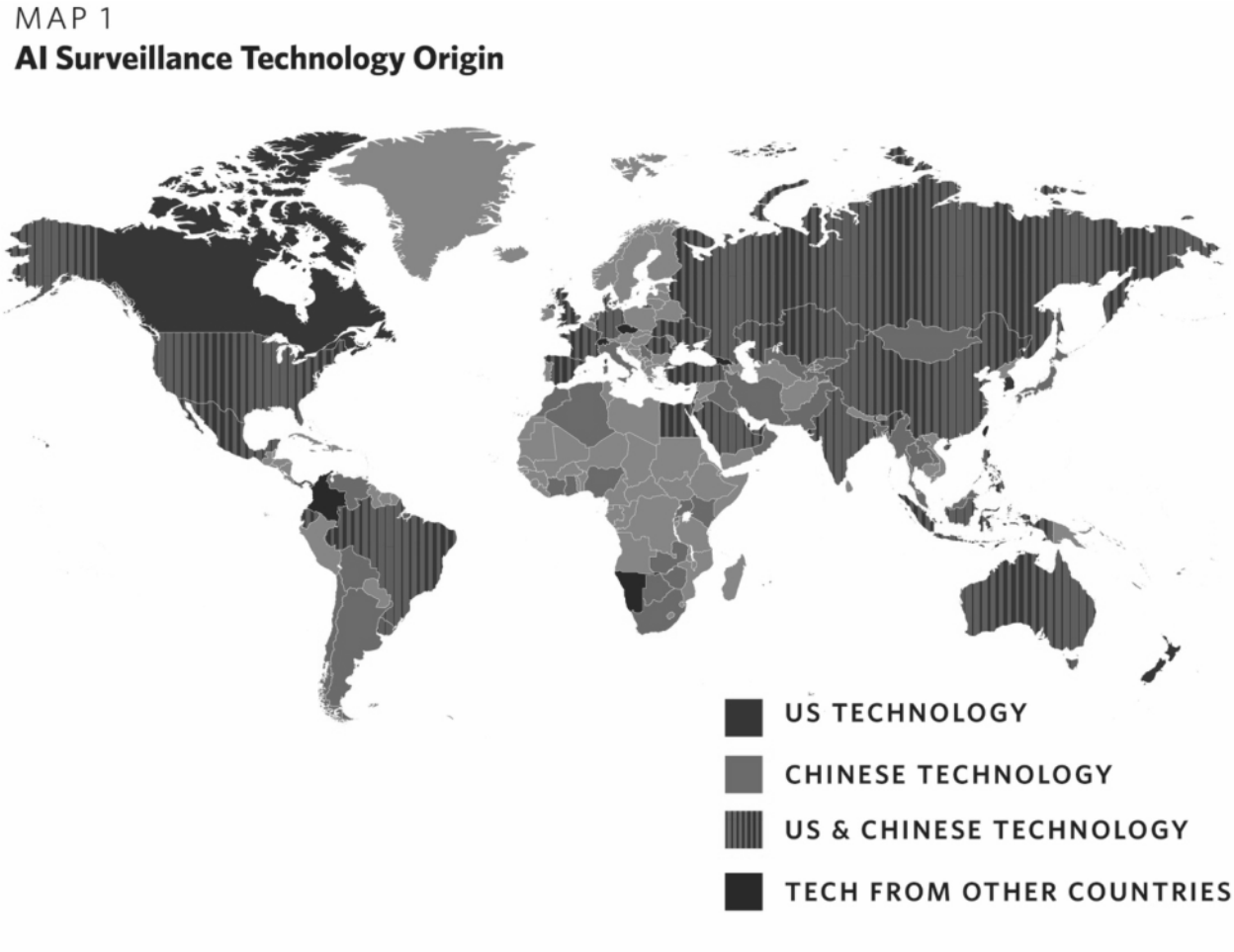
- Governments in autocratic and semi-autocratic countries are more prone to abuse AI surveillance than governments in liberal democracies. Some autocratic governments—for example, China, Russia, Saudi Arabia—are exploiting AI technology for mass surveillance purposes. Other governments with dismal human rights records are exploiting AI surveillance in more limited ways to reinforce repression. Yet all political contexts run the risk of unlawfully exploiting AI surveillance technology to obtain certain political objectives.

- There is a strong relationship between a country's military expenditures and a government's use of AI surveillance systems: forty of the world's top fifty military spending countries (based on cumulative military expenditures) also use AI surveillance technology.[2]

- The "Freedom on the Net 2018" report identified eighteen countries out of sixty-five that had accessed AI surveillance technology developed by Chinese companies.[3] The AIGS Index shows that the number of those countries accessing Chinese AI surveillance technology has risen to forty-seven out of sixty-five countries in 2019.

MAP 1

AI Surveillance Technology Origin



Notes:

- The AIGS Index presents a country-by-country snapshot of AI tech surveillance with the majority of sources falling between 2017 and 2019. Given the opacity of government surveillance use, it is nearly impossible to pin down by specific year which AI platforms or systems are currently in use.

- The AIGS Index uses the same list of independent states included in the Varieties of Democracy (V-Dem) project with two exceptions, totaling 176.[4] The V-Dem country list includes all independent polities worldwide but excludes microstates with populations below 250,000.

- The AIGS Index does not present a complete list of AI surveillance companies operating in particular countries. The paper uses open source reporting and content analysis to derive its findings. Accordingly, there are certain built-in limitations. Some companies, such as Huawei, may have an incentive to highlight new capabilities in this field. Other companies

have opted to downplay their association with surveillance technology and have purposely kept documents out of the public domain.

A full version of the index can be accessed online here:
https://carnegieendowment.org/files/AISurveillanceGlobalIndex.pdf
An interactive map keyed to the index that visually depicts the global spread of AI surveillance technology can be accessed here: https://carnegieendowment.org/AIGlobalSurveillance

All reference source material used to build the index has been compiled into an open Zotero library. It is available here: https://www.zotero.org/groups/2347403/global_ai_surveillance/items.

Introducing the AI Global Surveillance (AIGS) Index

AI technology was once relegated to the world of science fiction, but today it surrounds us. It powers our smartphones, curates our music preferences, and guides our social media feeds. Perhaps the most notable aspect of AI is its sudden ubiquity.

In general terms, the goal of artificial intelligence is to "make machines intelligent" by automating or replicating behavior that "enables an entity to function appropriately and with foresight in its environment," according to computer scientist Nils Nilsson.[5] AI is not one specific technology. Instead, it is more accurate to think of AI as an integrated system that incorporates information acquisition objectives, logical reasoning principles, and self-correction capacities. An important AI subfield is machine learning, which is a statistical process that analyzes a large amount of information in order to discern a pattern to explain the current data and predict future uses.[6] Several breakthroughs are making new achievements in the field possible: the maturation of machine learning and the onset of deep learning; cloud computing and online data gathering; a new generation of advanced microchips and computer hardware; improved performance of complex algorithms; and market-driven incentives for new uses of AI technology.[7]

Unsurprisingly, AI's impact extends well beyond individual consumer choices. It is starting to transform basic patterns of governance, not only by providing governments with unprecedented capabilities to monitor their citizens and shape their choices but also by giving them new capacity to disrupt elections, elevate false information, and delegitimize democratic discourse across borders.

The focus of this paper is on AI surveillance and the specific ways governments are harnessing a multitude of tools—from facial recognition systems and big data platforms to predictive policing algorithms—to advance their political goals. Crucially, the index does not distinguish between AI surveillance used for legitimate purposes and unlawful digital surveillance. Rather, the purpose of the research is to shine a light on new surveillance capabilities that are transforming the ability of states—from autocracies to advanced democracies—to keep watch on individuals.

AIGS Index—Methodology

The AIGS Index provides a detailed empirical picture of global AI surveillance trends and describes how governments worldwide are using this technology. It addresses three primary questions:

- Which countries are adopting AI surveillance technology?
- What specific types of AI surveillance are governments deploying?
- Which countries and companies are supplying this technology?

The AIGS Index is contained in Appendix 1. It includes detailed information for seventy-five countries where research indicates governments are deploying AI surveillance technology. The index breaks down AI surveillance tools into the following subcategories: 1) smart city/safe city, 2) facial recognition systems, and 3) smart policing. A full version of the index can be accessed online at https://carnegieendowment.org/files/AIGlobalSurveillanceIndex.pdf. An interactive map keyed to the index that visually depicts the global spread of AI surveillance technology can be accessed at https://carnegieendowment.org/AIGlobalSurveillance

All reference source material used to build the index has been compiled into an open Zotero library. It is available at https://www.zotero.org/groups/2347403/global_ai_surveillance/items.

The majority of sources referenced by the index occur between 2017 and 2019. A small number of sources date as far back as 2012. The index uses the same list of countries found in the Varieties of Democracy (V-Dem) project with two minor exceptions.[8] The V-Dem country list includes all independent polities worldwide but excludes microstates with populations below 250,000. The research collection effort combed through open-source material, country by country, in English and other languages, including news articles, websites, corporate documents, academic articles, NGO reports, expert submissions, and other public sources. It relied on systematic content analysis for each country incorporating multiple sources to determine the presence of relevant AI surveillance technology and corresponding companies. Sources were categorized into tiered levels of reliability and accuracy. First-tier sources include major print and news magazine outlets (such as the *New York Times*, *Economist*, *Financial Times*, and *Wall Street Journal*). Second-tier sources include major national media outlets. Third-tier sources include web articles, blog posts, and other less substantiated sourcing; these were only included after multiple corroboration.

Given limited resources and staffing constraints (one full-time researcher plus volunteer research assistance), the index is only able to offer a snapshot of AI surveillance levels in a given country. It does not provide a comprehensive assessment of all relevant technology, government surveillance uses, and applicable companies. Because research relied primarily on content analysis and literature reviews to derive its findings, there are certain built-in limitations. Some companies, such as Huawei, may have an incentive to highlight new capabilities in this field. Other companies may wish to downplay links to surveillance technology and purposely keep documents out of the public domain.

Field-based research involving on-the-ground information collection and verification would be useful to undertake. A number of countries—such as Angola, Azerbaijan, Belarus, Hungary, Peru, Sri Lanka, Tunisia, and Turkmenistan—provided circumstantial or anecdotal evidence of AI surveillance, but not enough verifiable data to warrant inclusion in the index.

A major difficulty was determining which AI technologies should be included in the index. AI technologies that directly support surveillance objectives—smart city/safe city platforms, facial recognition systems, smart policing systems—are included in the index. Enabling technologies that are critical to AI functioning but not directly responsible for surveillance programs are not included in the index.

Another data collection challenge is that governments (and many companies) purposely hide their surveillance capabilities. As such, it is difficult to precisely determine the extent to which states are deploying algorithms to support their surveillance objectives, or whether AI use is more speculative than real.

The index does not differentiate between governments that expansively deploy AI surveillance techniques versus those that use AI surveillance to a much lesser degree (for example, the index does not include a standardized interval scale correlating to levels of AI surveillance). This is by design. Because this is a nascent field and there is scant information about how different countries are using AI surveillance techniques, attempting to score a country's relative use of AI surveillance would introduce a significant level of researcher bias. Instead, a basic variable was used: is there documented presence of AI surveillance in a given country? If so, what types of AI surveillance technology is the state deploying? Future research may be able to assess and analyze levels of AI surveillance on a cross-comparative basis.

Finally, instances of AI surveillance documented in the index are not specifically tied to harmful outcomes. The index does not differentiate between unlawful and legitimate surveillance. In part, this is because it is exceedingly difficult to determine what specifically governments are doing in the surveillance realm and what the associated impacts are; there is too much that is unknown and hidden.

Findings and Three Key Insights

The findings indicate that at least seventy-five out of 176 countries globally are actively using AI technologies for surveillance purposes. This includes: smart city/safe city platforms (fifty-six countries), facial recognition systems (sixty-four countries), and smart policing (fifty-two countries). Three key insights emerge from the AIGS Index's findings.

First, global adoption of AI surveillance is increasing at a rapid pace around the world. Seventy-five countries, representing 43 percent of total countries assessed, are deploying AI-powered surveillance in both lawful and unlawful ways. The pool of countries is heterogeneous—they come from all

regions, and their political systems range from closed autocracies to advanced democracies. The "Freedom on the Net 2018" report raised eyebrows when it reported that eighteen out of sixty-five assessed countries were using AI surveillance technology from Chinese companies.[9] The report's assessment period ran from June 1, 2017 to May 31, 2018. One year later, the AIGS Index finds that forty-seven countries out of that same group are now deploying AI surveillance technology from China.

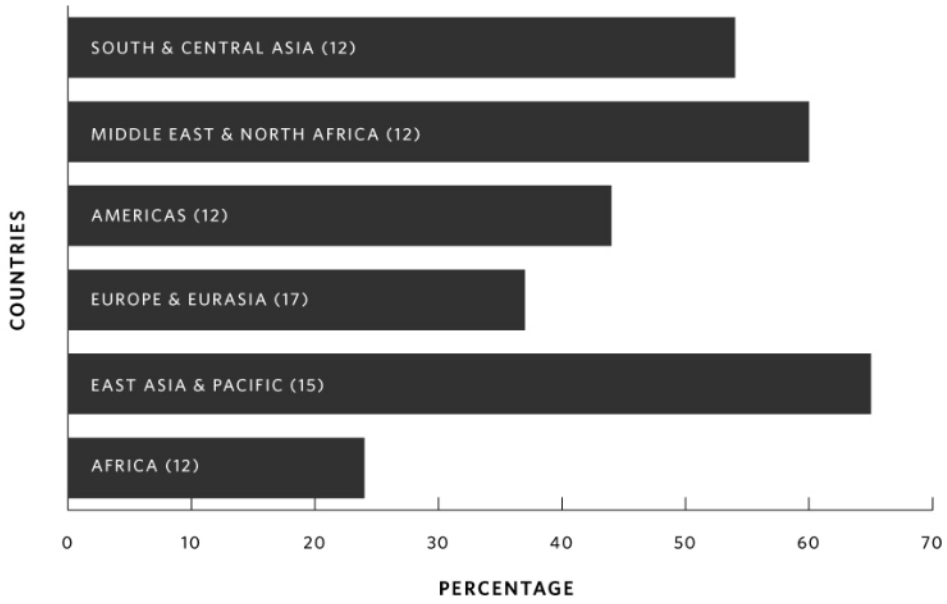
Unsurprisingly, countries with authoritarian systems and low levels of political rights are investing heavily in AI surveillance techniques. Many governments in the Gulf, East Asia, and South/Central Asia are procuring advanced analytic systems, facial recognition cameras, and sophisticated monitoring capabilities. But liberal democracies in Europe are also racing ahead to install automated border controls, predictive policing, safe cities, and facial recognition systems. In fact, it is striking how many safe city surveillance case studies posted on Huawei's website relate to municipalities in Germany, Italy, the Netherlands, and Spain.

Regionally, there are clear disparities. The East Asia/Pacific and the Middle East/North Africa regions are robust adopters of these tools. South and Central Asia and the Americas also demonstrate sizable take-up of AI surveillance instruments. Sub-Saharan Africa is a laggard—less than one-quarter of its countries are invested in AI surveillance. Most likely this is due to technological underdevelopment (African countries are struggling to extend broadband access to their populations; the region has eighteen of twenty countries with the lowest levels of internet penetration).[10] Given the aggressiveness of Chinese companies to penetrate African markets via BRI, these numbers will likely rise in the coming years. Figure 1 shows the percentage breakdown by region of countries adopting AI surveillance.

Second, China is a major supplier of AI surveillance. Technology linked to Chinese companies are found in at least sixty-three countries worldwide. Huawei alone is responsible for providing AI surveillance technology to at least fifty countries. There is also considerable overlap between China's Belt and Road Initiative and AI surveillance—thirty-six out of eighty-six BRI countries also contain significant AI surveillance technology. However, China is not the only country supplying advanced surveillance technology. France, Germany, Japan, and the United States are also major players in this sector. U.S. companies, for example, have an active presence in thirty-two countries. Figure 2 breaks down the leading companies in the sector.

FIGURE 1

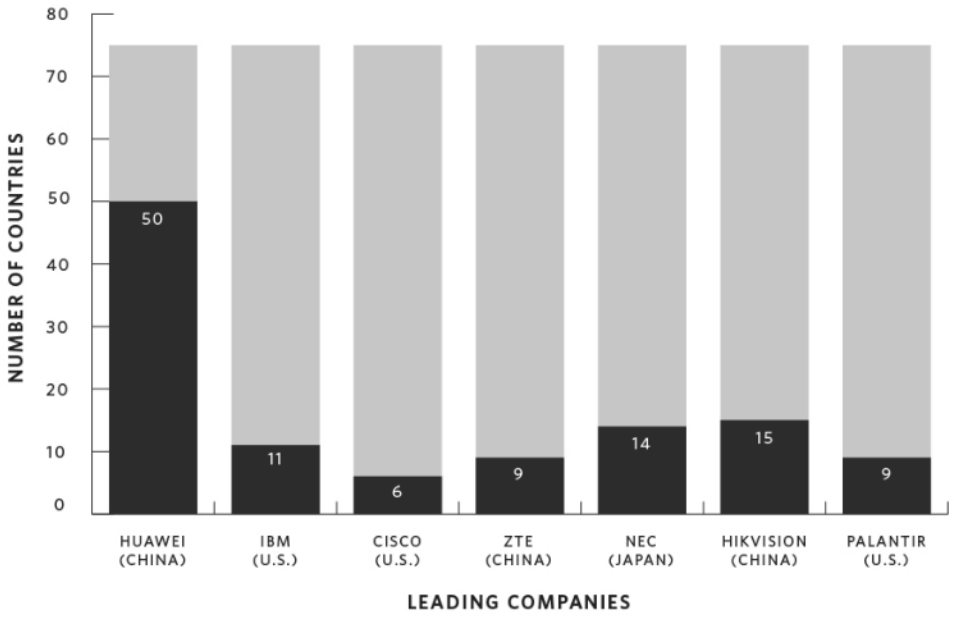
Percentage of Countries by Region Adopting AI Surveillance



NOTE: The numbers in parentheses indicate how many countries per region have adopted AI surveillance.

FIGURE 2

Leading Companies Contributing to AI Surveillance



NOTE: The AIGS Index tracks seventy-five countries that employ AI surveillance. The numbers here reflect how many of those countries each company is present in.

Third, liberal democracies are major users of AI surveillance. The index shows that 51 percent of advanced democracies deploy AI surveillance systems. In contrast, 37 percent of closed autocratic states, 41 percent of electoral autocratic/competitive autocratic states, and 41 percent of electoral democracies/illiberal democracies deploy AI surveillance technology. Liberal democratic governments are aggressively using AI tools to police borders, apprehend potential criminals, monitor citizens for bad behavior, and pull out suspected terrorists from crowds. This doesn't necessarily mean that democracies are using this technology unlawfully. The most important factor determining whether governments will exploit this technology for repressive purposes is the quality of their governance—is there an existing pattern of human rights violations? Are there strong rule of law traditions and independent institutions of accountability? That should provide a measure of reassurance for citizens residing in democratic states.

But advanced democracies are struggling to balance security interests with civil liberties protections. In the United States, increasing numbers of cities have adopted advanced surveillance systems. A 2016 investigation by Axios's Kim Hart revealed, for example, that the Baltimore police had secretly deployed aerial drones to carry out daily surveillance over the city's residents: "From a plane flying overhead, powerful cameras capture aerial images of the entire city. Photos are snapped every second, and the plane can be circling the city for up to 10 hours a day."[11] Baltimore's police also deployed facial recognition cameras to monitor and arrest protesters, particularly during 2018 riots in the city.[12] The ACLU condemned these techniques as the "technological equivalent of putting an ankle GPS [Global Positioning Service] monitor on every person in Baltimore."[13]

On the U.S.-Mexico border, an array of hi-tech companies also purvey advanced surveillance equipment. Israeli defense contractor Elbit Systems has built "dozens of towers in Arizona to spot people as far as 7.5 miles away," writes the *Guardian*'s Olivia Solon. Its technology was first perfected in Israel from a contract to build a "smart fence" to separate Jerusalem from the West Bank. Another company, Anduril Industries, "has developed towers that feature a laser-enhanced camera, radar and a communications system" that scans a two-mile radius to detect motion. Captured images "are analysed using artificial intelligence to pick out humans from wildlife and other moving objects."[14] It is unclear to what extent these surveillance deployments are covered in U.S. law, let alone whether these actions meet the necessity and proportionality standard.

The United States is not the only democracy embracing AI surveillance. In France, the port city of Marseille initiated a partnership with ZTE in 2016 to establish the Big Data of Public Tranquility project. The goal of the program is to reduce crime by establishing a vast public surveillance network featuring an intelligence operations center and nearly one thousand intelligent closed-circuit television (CCTV) cameras (the number will double by 2020). Local authorities trumpet that this system will make Marseille "the first 'safe city' of France and Europe."[15] Similarly, in 2017, Huawei

"gifted" a showcase surveillance system to the northern French town of Valenciennes to demonstrate its safe city model. The package included upgraded high definition CCTV surveillance and an intelligent command center powered by algorithms to detect unusual movements and crowd formations.[16]

The fact that so many democracies—as well as autocracies—are taking up this technology means that regime type is a poor predictor for determining which countries will adopt AI surveillance.

A better predictor for whether a government will procure this technology is related to its military spending. A breakdown of military expenditures in 2018 shows that forty of the top fifty military spending countries also have AI surveillance technology.[17] These countries span from full democracies to dictatorial regimes (and everything in between). They comprise leading economies like France, Germany, Japan, and South Korea, and poorer states like Pakistan and Oman. This finding is not altogether unexpected; countries with substantial investments in their militaries tend to have higher economic and technological capacities as well as specific threats of concern. If a country takes its security seriously and is willing to invest considerable resources in maintaining robust military-security capabilities, then it should come as little surprise that the country will seek the latest AI tools. The motivations for why European democracies acquire AI surveillance (controlling migration, tracking terrorist threats) may differ from Egypt or Kazakhstan's interests (keeping a lid on internal dissent, cracking down on activist movements before they reach critical mass), but the instruments are remarkably similar. Future research might examine country-level internal security figures and compare them to levels of AI surveillance.

Distinguishing Between Legitimate and Unlawful Surveillance

State surveillance is not inherently unlawful. Governments have legitimate reasons to undertake surveillance that is not rooted in a desire to enforce political repression and limit individual freedoms. For example, tracking tools play a vital role in preventing terrorism. They help security forces deter bad acts and resolve problematic cases. They give authorities the ability to monitor critical threats and react accordingly. But technology has changed the nature of how governments carry out surveillance and what they choose to monitor. The internet has proliferated the amount of transactional data or "metadata" available about individuals, such as information about sent and received emails, location identification, web-tracking, and other online activities. As former UN special rapporteur Frank La Rue noted in a milestone 2013 surveillance report:

> Communications data are storable, accessible and searchable, and their disclosure to and use by State authorities are largely unregulated. Analysis of this data can be both highly revelatory and invasive, particularly when data is combined and aggregated. As such, States

> are increasingly drawing on communications data to support law enforcement or national security investigations. States are also compelling the preservation and retention of communication data to enable them to conduct historical surveillance.[18]

It goes without saying that such intrusions profoundly affect an individual's right to privacy—to not be subjected to what the Office of the UN High Commissioner for Human Rights (OHCHR) called "arbitrary or unlawful interference with his or her privacy, family, home or correspondence."[19] Surveillance likewise may infringe upon an individual's right to freedom of association and expression. Under international human rights law, three principles are critical to assessing the lawfulness of a particular surveillance action.

First, does domestic law allow for surveillance? La Rue's successor, David Kaye, issued a report in 2019 that affirmed that legal regulations should be "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public." Legal requirements should not be "vague or overbroad," which would allow unconstrained discretion to government officials. The legal framework itself should be "publicly accessible, clear, precise, comprehensive and non-discriminatory."[20]

Second, does the surveillance action meet the "necessity and proportionality" international legal standard, which restricts surveillance to situations that are "strictly and demonstrably necessary to achieve a legitimate aim"?[21]

Third, are the interests justifying the surveillance action legitimate? Disagreements abound when it comes to determining what constitutes legitimate surveillance and what is an abuse of power. While governments commonly justify surveillance on national security or public order grounds, the OHCHR warns that such restrictions may "unjustifiably or arbitrarily" restrict citizens' rights to freedom of opinion and expression. It contends that legitimate surveillance requires states to "demonstrate the risk that specific expression poses to a definite interest in national security or public order," and that a "robust, independent oversight system" that entrusts judiciaries to authorize relevant surveillance measures and provide remedies in cases of abuse is required.[22] Kaye adds that legitimate surveillance should only apply when the interest of a "whole nation is at stake," and should exclude surveillance carried out "in the sole interest of a Government, regime or power group."[23]

The legal standards required to legitimately carry out surveillance are high, and governments struggle to meet them. Even democracies with strong rule of law traditions and robust oversight institutions frequently fail to adequately protect individual rights in their surveillance programs. Countries with weak legal enforcement or authoritarian systems "routinely shirk these obligations."[24] As the OHCHR's inaugural report on privacy in the digital age concludes, states with "a lack of adequate

national legislation and/or enforcement, weak procedural safeguards and ineffective oversight" bring reduced accountability and heightened conditions for unlawful digital surveillance.[25]

AI surveillance exacerbates these conditions and makes it likelier that democratic and authoritarian governments may carry out surveillance that contravenes international human rights standards. Frank La Rue explains: "Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."[26]

AI surveillance in particular offers governments two major capabilities. One, AI surveillance allows regimes to automate many tracking and monitoring functions formerly delegated to human operators. This brings cost efficiencies, decreases reliance on security forces, and overrides potential principal-agent loyalty problems (where the very forces operating at the behest of the regime decide to seize power for themselves).

Two, AI technology can cast a much wider surveillance net than traditional methods. Unlike human operatives "with limited reserves of time and attention," AI systems never tire or fatigue.[27] As a result, this creates a substantial "chilling effect" even without resorting to physical violence; citizens never know if an automated bot is monitoring their text messages, reading their social media posts, or geotracking their movements around town.[28]

This paper recognizes that AI surveillance technology is "value neutral." In and of themselves, these tools do not foment repression, and their presence does not mean that a government is using them for antidemocratic purposes. The index does not specify, country-by-country, whether these instruments are being used by governments in lawful or illegitimate manners. Rather, the purpose of the index is to identify which countries possess sufficiently advanced tools that allow them to pursue a range of surveillance objectives.

How Much Is China Driving the Spread of AI Surveillance?

Empirically, the AIGS Index shows that Chinese companies—led by Huawei—are leading suppliers of AI surveillance around the world. Overall, China is making a sustained push for leadership and primacy in AI.[29] A growing consensus singles out China as a global driver of "authoritarian tech." Experts claim that Chinese companies are working directly with Chinese state authorities to export "authoritarian tech" to like-minded governments in order to spread influence and promote an alternative governance model.[30] But is this accurate?

There is some truth to this argument—a subset of Chinese exports goes directly to countries like Zimbabwe and Venezuela that are gross human rights violators and which would otherwise be unable to access such technology. But AI surveillance is not solely going from one authoritarian country (China) to other authoritarian states. Rather, transfers are happening in a much more heterogeneous fashion. China is exporting surveillance tech to liberal democracies as much as it is targeting authoritarian markets. Likewise, companies based in liberal democracies (for example, Germany, France, Israel, Japan, South Korea, the UK, the United States) are actively selling sophisticated equipment to unsavory regimes.

Saudi Arabia is a good case in point. Huawei is helping the government build safe cities, but Google is establishing cloud servers, UK arms manufacturer BAE has sold mass surveillance systems, NEC is vending facial recognition cameras, and Amazon and Alibaba both have cloud computing centers in Saudi Arabia and may support a major smart city project.[31] The index shows that repressive countries rarely procure such technology from a single source. In Thailand, government officials repeatedly emphasized the importance of "foreign policy balancing" and not affiliating too strongly with any one side: "Always been that way. That's why we're still a kingdom. We compromise, we negotiate, and we balance."[32]

That being said, there are special reasons why experts are applying greater scrutiny to Chinese companies. Huawei is the leading vendor of advanced surveillance systems worldwide by a huge factor. Its technology is linked to more countries in the index than any other company. It is aggressively seeking new markets in regions like sub-Saharan Africa. Huawei is not only providing advanced equipment but also offering ongoing technological support to set up, operate, and manage these systems.

A recent investigative report by the *Wall Street Journal* provides an eye-opening example. The reporters found that Huawei technicians in both Uganda and Zambia helped government officials spy on political opponents. This included "intercepting their encrypted communications and social media, and using cell data to track their whereabouts." Not only did Huawei employees play a "direct role in government efforts to intercept the private communications of opponents," but they also encouraged Ugandan security officials to travel to Algeria so they could study Huawei's "intelligent video surveillance system" operating in Algiers.[33] Uganda subsequently agreed to purchase a similar facial recognition surveillance system from Huawei costing $126 million.[34]

The Australian Strategic Policy Institute's project on Mapping China's Tech Giants indicates that Huawei is responsible for seventy-five "smart city-public security projects," and has seen a colossal increase in its business line: "In 2017, Huawei listed 40 countries where its smart-city technologies had been introduced; in 2018, that reach had reportedly more than doubled to 90 countries (including 230 cities)."[35] Huawei is directly pitching the safe city model to national security agencies,

and China's Exim Bank appears to be sweetening the deal with subsidized loans. The result is that a country like Mauritius obtains long-term financing from the Chinese government, which mandates contracting with Chinese firms.[36] The Mauritian government then turns to Huawei as the prime contractor or sub-awardee to set up the safe city and implement advanced surveillance controls.

It is also increasingly clear that firms such as Huawei operate with far less independence from the Chinese government than they claim. Huawei was founded in 1987 by Ren Zhengfei, a former officer in the People's Liberation Army who served in its "military technology division," Anna Fifield at the *Washington Post* has noted.[37] There are consistent reports that Huawei receives significant subsidies from the Chinese government.[38] There also appear to be strong connections between Huawei's leadership and China's security and intelligence apparatus. Sun Yafang, for example, chairwoman of Huawei's board from 1999 to 2018, once worked in China's Ministry of State Security.[39] Max Chafkin and Joshua Brustein reported in *Bloomberg Businessweek* that there are allegations that Ren may have been a "high-ranking Chinese spymaster and indeed may still be."[40] Experts maintain that the Chinese Communist Party increasingly is establishing "party 'cells' in private companies to enable enhanced access and control.[41] Huawei has publicly averred that it would "definitely say no" to any demands by the Chinese government to hand over user data.[42] But this contravenes a 2015 Chinese national security law that mandates companies to allow third-party access to their networks and to turn over source code or encryption keys upon request.[43] Huawei's declared ownership structure is remarkably opaque. A recent academic study by Christopher Balding and Donald C. Clarke concluded that 99 percent of Huawei shares are controlled by a "trade union committee," which in all likelihood is a proxy for Chinese state control of the company."[44]

Even if Chinese companies are making a greater push to sell advanced surveillance tech, the issue of intentionality remains perplexing—to what extent are Chinese firms like Huawei and ZTE operating out of their own economic self-interest when peddling surveillance technology versus carrying out the bidding of the Chinese state? At least in Thailand, recent research interviews did not turn up indications that Chinese companies are pushing a concerted agenda to peddle advanced AI surveillance equipment or encourage the government to build sophisticated monitoring systems. An official from Thailand's Ministry of Interior noted that while AI technology is "out there" and something the government is thinking more about, "China hasn't offered any AI. It doesn't give AI—Thais have to ask."[45] The smart city/safe city model also garnered skepticism. Somkiat Tangkitvanich, a leading technology expert in Thailand, commented, "the idea of a smart city is a joke." He relayed a recent conversation he had with Thailand's information and communications technologies (ICT) minister: "He [the minister] boasted about the smart city in Phuket. . . . He told me that we are thinking about giving wristbands to tourists so that we can track them, we can help them. Something like that. But it's not really implemented. Smart city in Phuket turns out to be providing free Wi-Fi and internet to tourists!"[46] This serves as a useful reminder that more on-the-ground research is needed to separate hyperbole from fact in this area.

Types of AI Surveillance

The following sections will describe key AI surveillance techniques and how governments worldwide are deploying them to support specific policy objectives.

States use AI technology to accomplish a broad range of surveillance goals. This section details three primary AI surveillance tools incorporated in the AIGS Index: smart city/safe city platforms, facial recognition systems, and smart policing. It also describes enabling technologies—such as cloud computing and Internet of Things (IOT) networks—that are integral for AI surveillance tools to function. Enabling technologies are not incorporated in the index.

Importantly, AI surveillance is not a standalone instrument of repression. It forms part of a suite of digital repression tools—information and communications technologies used to surveil, intimidate, coerce, and harass opponents in order to inflict a penalty on a target and deter specific activities or beliefs that challenge the state.[47] (See Appendix 2 for more information.) Table 1 summarizes each technique and its corresponding level of global deployment.

TABLE 1

Summary of AI Surveillance Techniques and Global Prevalence

AI Surveillance Technique	Description	Global Proliferation (out of 75 countries)
Smart Cities/Safe Cities	Cities with sensors that transmit real-time data to facilitate service delivery, city management, and public safety. Often referred to as "safe cities," they incorporate sensors, facial recognition cameras, and police body cameras connected to intelligent command centers to prevent crime, ensure public safety, and respond to emergencies. Only platforms with a clear public safety focus are incorporated in the index.	56 countries
Facial Recognition Systems	Biometric technology that uses cameras (still images or video) to match stored or live footage of individuals with images from databases. Not all systems focus on database matching; some systems assess aggregate demographic trends or conduct broader sentiment analysis via facial recognition crowd scanning.	64 countries
Smart Policing	Data-driven analytic technology used to facilitate investigations and police response; some systems incorporate algorithmic analysis to make predictions about future crimes.	53 countries

Smart Cities/Safe Cities

The World Bank describes smart cities as "technology-intensive" urban centers featuring an array of sensors that gather information in real time from "thousands of interconnected devices" in order to facilitate improved service delivery and city management.[48] They help municipal authorities manage traffic congestion, direct emergency vehicles to needed locations, foster sustainable energy use, and streamline administrative processes. But there is growing concern that smart cities are also enabling a dramatic increase in public surveillance and intrusive security capabilities. IBM, one of the original coiners of the term, designed a brain-like municipal model where information relevant to city operations could be centrally processed and analyzed.[49] A key component of IBM's smart city is public safety, which incorporates an array of sensors, tracking devices, and surveillance technology to increase police and security force capabilities.

Huawei has been up-front about trumpeting public safety technologies for smart cities. It is marketing "safe cities" to law enforcement communities to "predict, prevent, and reduce crime" and "address new and emerging threats."[50] In a 2016 white paper, Huawei describes a "suite of technology that includes video surveillance, emergent video communication, integrated incident command and control, big data, mobile, and secured public safety cloud" to support local law enforcement and policing as well as the justice and corrections system.[51] Huawei explicitly links its safe city technology to confronting regional security challenges, noting that in the Middle East, its platforms can prevent "extremism"; in Latin America, safe cities enable governments to reduce crime; and that in North America, its technology will help the United States advance "counterextremism" programs.[52]

How do these platforms work in practice to advance surveillance goals? The IT firm Gartner, which partners with Microsoft on smart cities, provides an example:

> Saudi Arabia's Makkah Region Development Authority (MRDA) created a crowd-control system to increase safety and security of Hajj pilgrims. Data is collected via a wristband embedding identity information, special healthcare requirements and a GPS. In addition, surveillance cameras are installed to collect and analyze real-time video along the Al Mashaaer Al Mugaddassah Metro Southern Line (MMMSL), as well as in the holy sites, such as Great Mosque of Mecca, Mount Arafat, Jamarat and Mina.[53]

Unsurprisingly, such systems lend themselves to improper use. Recently, Huawei's safe city project in Serbia, which intends to install 1,000 high-definition (HD) cameras with facial recognition and license plate recognition capabilities in 800 locations across Belgrade, sparked national outrage.[54] Huawei posted a case study (since removed) about the benefits of safe cities and described how similar surveillance technology had facilitated the apprehension of a Serbian hit-and-run perpetrator who had fled the country to a city in China: "Based on images provided by Serbian police, the . . .

[local] Public Security Bureau made an arrest within three days using new technologies."[55] Rather than applaud the efficiency of the system, Serbian commentators observed that in a country racked by endemic corruption and encroaching authoritarianism, such technology offers a powerful tool for Serbian authorities to curb dissent and perpetrate abuses.

Smart city platforms with a direct public security link are found in at least fifty-six of seventy-five countries with AI surveillance technology.

Facial Recognition Systems

Facial recognition is a biometric technology that uses cameras—both video or still images—to match stored or live footage of individuals with images from a database. Not all facial recognition systems focus on individual identification via database matching. Some systems are designed to assess aggregate demographic trends or to conduct broader sentiment analysis via facial recognition crowd scanning.

Unlike ordinary CCTV, which has been a mainstay of police forces for twenty-five years, facial recognition cameras are much more intrusive. They can scan distinctive facial features in order to create detailed biometric maps of individuals without obtaining consent. Often facial recognition surveillance cameras are mobile and concealable. For example, security forces in Malaysia have entered into a partnership with the Chinese tech company Yitu to equip officers with facial recognition body cameras. This will allow security officials to "rapidly compare images caught by live body cameras with images from a central database."[56]

Huawei is a major purveyor of facial recognition video surveillance, particularly as part of its safe city platforms. It describes the technology's benefits in the Kenya Safe City project:

> As part of this project, Huawei deployed 1,800 HD cameras and 200 HD traffic surveillance systems across the country's capital city, Nairobi. A national police command center supporting over 9,000 police officers and 195 police stations was established to achieve monitoring and case-solving. The system worked during Pope Francis' visit to Kenya in 2015, where more than eight million people welcomed his arrival. With Huawei's HD video surveillance and a visualized integrated command solution, the efficiency of policing efforts as well as detention rates rose significantly.[57]

Experts detail several concerns associated with facial recognition.

First, few rules govern access to and the use of image databases (repositories that store captured images from facial recognition cameras). How governments use this information, how long images are stored, and where authorities obtain such images in the first place are opaque issues and vary by

jurisdiction. Recent disclosures that U.S. law enforcement agencies (the Federal Bureau of Investigation and Immigration and Customs Enforcement) scanned through millions of photos in state driver's license databases without prior knowledge or consent come as little surprise. The vacuum of legal checks and balances has led to a "surveillance-first, ask-permission-later system," Drew Harrell noted in the *Washington Post*.[58]

Second, the accuracy of facial recognition technology varies significantly. Certain tests have disclosed unacceptably high false-match rates. A recent independent report of the UK's Metropolitan Police found that its facial recognition technology had an extraordinary error rate of 81 percent.[59] Similarly, Axon, a leading supplier of police body cameras in the United States, announced that it would cease offering facial recognition on its devices. Axon's independent ethics board stated: "Face recognition technology is not currently reliable enough to ethically justify its use."[60]

But other assessments demonstrate much more favorable results. Evaluations conducted between 2014 and 2018 of 127 algorithms from thirty-nine developers by the U.S. National Institute for Standards and Technology showed that "facial recognition software got 20 times better at searching a database to find a matching photograph." The failure rate in the same period dropped from 4.0 percent to 0.2 percent.[61]

One reason for the discrepancy is that under ideal conditions, facial recognition can perform very well. But when unexpected variables are thrown in—poor weather or fuzzy database images—then failure rates start to shoot up. Facial recognition technology also has been unable to shake consistent gender and racial biases, which lead to elevated false positives for minorities and women—"the darker the skin, the more errors arise—up to nearly 35 percent for images of darker skinned women" noted Steve Lohr in the *New York Times*.[62]

Citizens are starting to fight back against facial recognition systems. Protesters in Hong Kong, for example, have covered up their faces and disabled their smartphone facial recognition logins to prevent law enforcement access. They have also turned the tables on the police by taking pictures of unbadged officers and using facial recognition image searching to expose the officers' identities online.[63]

Facial recognition systems are rapidly spreading around the world. The index identifies at least sixty-four countries that are actively incorporating facial recognition systems in their AI surveillance programs.

Smart Policing

The idea behind smart policing is to feed immense quantities of data into an algorithm—geographic location, historic arrest levels, types of committed crimes, biometric data, social media feeds—in order to prevent crime, respond to criminal acts, or even to make predictions about future criminal activity. As Privacy International notes: "With the proliferation of surveillance cameras, facial recognition, open source and social media intelligence, biometrics, and data emerging from smart cities, the police now have unprecedented access to massive amounts of data." Therefore, one major component to smart policing is to create automated platforms that can disaggregate immense amounts of material, facilitate data coming in from multiple sources, and permit fine-tuned collection of individual information.

One area that has received considerable recent attention is predictive policing. The technique accelerated in the United States after the National Institute of Justice started issuing grants for pilot predictive policing projects in 2009. At its core, these programs claim to predict with remarkable accuracy, based on massive data aggregation, where future crimes will be committed and which individuals are likely to commit those crimes. Predictive policing has exploded in popularity. The PredPol predictive analytics program, for example, is deployed "by more than 60 police departments around the country."[64]

But there are growing concerns about algorithmic bias and prejudice, as well as the effectiveness of these predictions. Recent reporting by Caroline Haskins for *Vice* describes how PredPol's predictive crime forecasting algorithm operates. Predpol's software generates crime forecasts for police officers "on a scale as small as 500 by 500 square feet," which can pinpoint specific houses. It assumes that "certain crimes committed at a particular time are more likely to occur in the same place in the future."[65] PredPol reveals that "historical event datasets are used to train the algorithm for each new city (ideally 2 to 5 years of data). PredPol then updates the algorithm each day with new events as they are received from the department." New predictions are highlighted in special red boxes superimposed on Google Maps representing high-risk areas that warrant special attention from police patrols.[66] A key shortcoming in PredPol's methodology is that it generates future predictions based on data from past criminal activity and arrests. Certain minority neighborhoods that have suffered from "overpolicing" and biased police conduct show up with higher frequency in PredPol's dashboard. This may not represent fine-tuned algorithmic crime prediction as much as it involves the perpetuation of structurally biased policing.

China has enthusiastically embraced predictive policing as part of its Xinjiang crackdown. Human Rights Watch reports on the creation of an Integrated Joint Operations Platform (IJOP), which collects data from CCTV cameras, facial recognition devices, and "wifi sniffers" (devices that eavesdrop on activities or communications within wireless networks). IJOP procures additional data from license plates and identification cards scanned at checkpoints, as well as health, banking, and

legal records.[67] Chinese authorities are supplementing IJOP with mandatory DNA samples from all Xinjiang residents aged twelve to sixty-five.[68] This information is fed into IJOP computers, and algorithms sift through troves of data looking for threatening patterns. Once IJOP flags an individual, that person is picked up by security forces and detained for questioning.[69]

Smart policing techniques are used in at least fifty-three of seventy-five countries with AI surveillance.

AI Surveillance Enabling Technologies

A second category of technology is not directly responsible for supporting surveillance programs, but provides critical capabilities that are essential for implementing applications. Advanced video surveillance and facial recognition cameras could not function without cloud computing capabilities. As one expert put it, if video surveillance is the "eyes" then cloud services are the "brains" that "connect cameras and hardware to the cloud computing models via 5G networks."[70] However, cloud computing in isolation is not inherently oriented toward surveillance. Therefore, these secondary technologies are placed in an "enabling technologies" category and described below.[71] They are not included in the AIGS Index.

TABLE 2
AI Surveillance—Enabling Technologies

AI Surveillance Technique	Description
Automated Border Control (ABC) Systems	Biometric systems powered by facial recognition to automatically control airport or border access; can also include biometric passports and IDs
Cloud Computing	Infrastructural components, networks, and sensors that enable AI processing and operations (for example, cloud servers, data centers, IOT networks)
Internet of Things	Devices connected via the internet that allow data to be shared for analytic processing in the cloud
Other AI Technology	Other relevant AI technologies such as digital government, AI training centers, and AI research institutes

Automated Border Control Systems

These are found primarily in international airports and border crossings. According to the consulting firm Accenture, ABC systems use "multi-model biometric matching"—facial image recognition combined with e-passports or other biometric documents—to process passengers.[72] The process initiates when a passenger steps in front of a multi-camera wall. Digital mirrors located adjacent to the cameras attract passengers' eyes for image capture. A risk assessment is then performed through automated testing of identities against an individual's passport and certain security watch-lists.[73] Those who are not cleared by the automated system must go into secondary screening with human agents.

Governments are piloting new features, such as automated lie detection technology, in ABC systems. For example, the European Union is testing a technology called iBorderCtrl in three countries—Greece, Hungary, and Latvia—to screen migrants at border crossings. Individuals are asked questions about their countries of origin and circumstances of departure. The answers are then evaluated by an AI-based lie-detecting system.[74] Travelers found to have honestly answered questions are given a code allowing them to cross. All others are transferred to human border guards for additional questioning. The technology behind iBorderCtrl is based on "affect recognition science," which purports to read facial expressions and infer emotional states in order to render legal judgments or policy decisions. Psychologists have widely criticized these tools, maintaining that it is difficult to rely on facial expressions alone to accurately determine a person's state of mind.[75] Despite scientific skepticism about these techniques, governments continue to explore their use.

Cloud Computing

Governments and companies are increasingly storing data in massive off-site locations—known as the cloud—that are accessible through a network, usually the internet.[76] Cloud computing is a general use technology that includes everything from turn-by-turn GPS maps, social network and email communications, file storage, and streaming content access. The National Institute of Standards and Technology defines cloud computing as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[77] In basic terms, cloud computing data centers function as the backbone of the internet, instantly storing, communicating, and transporting produced information. As such, cloud computing is essential to effectively running AI systems. Microsoft, IBM, Amazon, Huawei, and Alibaba have all established these data centers to facilitate AI operations.

A growing number of countries have fully embraced cloud computing and outsourced all of their data storage needs to a single corporate platform. In 2018, for example, Iceland signed a service agreement with Microsoft for the company to be the sole IT supplier for the country's entire public

sector.[78] The cloud computing trend is not without problems. For one, cloud servers present enticing targets for cyber hackers. Security firms like NSO Group claim they are able to penetrate cloud servers and access a target's "location data, archived messages or photos," leading many to question whether cloud computing companies can keep personal information, corporate secrets, classified government material, or health records safe (however they generally represent a more secure method of storage than legacy on-site data storage facilities).[79] A related concern is forced data disclosures—even if cloud servers remain technically secure, governments may coerce companies into disclosing certain data (such as email communications or text messages of regime critics) held in the cloud.

Internet of Things

The IOT is based on the reality that more and more devices will be connected to each other via the internet, allowing data to be shared for analytic processing in the cloud.[80] A major IOT hurdle is lack of interoperability between devices. At present, iPhones, Alexa speakers, Nest thermostats, and OnStar auto systems function from different platforms and use different information sources. The IOT's goal is to "help tame this Tower of Babel" and ensure device integration and data aggregation (although companies like Amazon, Apple, and Google are also setting up distinct ecosystems that only have limited interoperability with other platforms).[81] While the IOT will bring greater efficiencies, it may also transform traditional non-networked devices, such as smart speakers, into omnipresent surveillance instruments:

> The Internet of Things promises a new frontier for networking objects, machines, and environments in ways that we [are] just beginning to understand. When, say, a television has a microphone and a network connection, and is reprogrammable by its vendor, it could be used to listen in to one side of a telephone conversation taking place in its room—no matter how encrypted the telephone service itself might be. These forces are on a trajectory towards a future with more opportunities for surveillance.[82]

Controversy surrounding IOT technology is growing. In early 2019, Amazon disclosed that thousands of its workers listened to conversations recorded by Echo smart speakers. In some cases, its workers debated whether recordings of possible crimes should be turned over to law enforcement authorities.[83] Amazon analyzed these transcripts without the knowledge or consent of its customers. Similarly, it came to light that Google and Facebook contractors have been regularly listening to recordings between their platforms and individual consumers.[84]

IOT-powered mobile surveillance is another possibility for this class of technology. A new device was recently demonstrated that plugs into a Tesla Model S or Model 3 car and turns its built-in cameras "into a system that spots, tracks, and stores license plates and faces over time," journalist Andy Greenberg described. When the owner has parked the car, "it can track nearby faces to see which ones repeatedly appear." The purpose of the device is to warn car owners against thieves and vandals.

But as the device's inventor Truman Kain acknowledges, "it turns your Tesla into an AI-powered surveillance station" and provides "another set of eyes, to help out and tell you it's seen a license plate following you over multiple days, or even multiple turns of a single trip."[85]

Conclusion

The spread of AI surveillance continues unabated. Its use by repressive regimes to engineer crackdowns against targeted populations has already sounded alarm bells. But even in countries with strong rule of law traditions, AI gives rise to troublesome ethical questions. Experts express concerns about facial recognition error rates and heightened false positives for minority populations. The public is increasingly aware about algorithmic bias in AI training datasets and their prejudicial impact on predictive policing algorithms and other analytic tools used by law enforcement. Even benign IOT applications—smart speakers, remote keyless entry locks, automotive intelligent dash displays—may open troubling pathways for surveillance. Pilot technologies that states are testing on their borders—such as iBorderCtrl's affective recognition system—are expanding despite criticisms that they are based on faulty science and unsubstantiated research. The cumulative impact gives pause. Disquieting questions are surfacing regarding the accuracy, fairness, methodological consistency, and prejudicial impact of advanced surveillance technologies. Governments have an obligation to provide better answers and fuller transparency about how they will use these new intrusive tools.

The purpose of the index and working paper is to highlight emergent trends for a technology that is not well understood yet will increasingly shape modern life. The good news is that there is ample time to initiate a much-needed public debate about the proper balance between AI technology, government surveillance, and the privacy rights of citizens. But as these technologies become more embedded in governance and politics, the window for change will narrow.

Appendix 1

AIGS Index

CA Closed Autocracy
EA Electoral Autocracy/Competitive Autocracy
ED Electoral Democracy/Illiberal Democracy
LD Liberal Democracy

Country	Regime Type	"Freedom on the Net 2018" Status	Military Spending Ranking (2018)	BRI Country?	Smart/ Safe City?	Facial Recognition?	Smart Policing?	Chinese Tech?	U.S. Tech?	Key Companies
Algeria	EA		25				✓	✓		BAE, Huawei
Argentina	ED	FREE	43			✓	✓	✓		Axis, Bosch, Dahua, Huawei, NEC, ZTE
Armenia	EA	FREE	81	✓	✓	✓		✓		Hikvision, Huawei
Australia	LD	FREE	13		✓	✓	✓	✓	✓	CrowdOptic, Hikvision, Huawei, Infinova, NEC, Palantir
Bahrain	CA	NOT FREE	65	✓		✓	✓	✓		Dahua
Bangladesh	EA	PARTLY FREE	44	✓	✓	✓	✓	✓		Huawei
Bolivia	ED		79	✓	✓	✓	✓	✓		CEIEC, Huawei, ZTE
Botswana	ED		86		✓		✓	✓		Huawei
Brazil	ED	PARTLY FREE	12		✓	✓	✓	✓	✓	Axis, Dahua, IBM
Burma/ Myanmar	EA	NOT FREE	58	✓	✓	✓		✓		Hikvision, Huawei
Canada	LD	FREE	14			✓	✓		✓	Avigilon, Palantir
Chile	LD		34			✓	✓	✓		Huawei
China	CA	NOT FREE	2		✓	✓	✓	✓	✓	Mult; Axis, Bosch, IBM, Microsoft, Seagate, Qualcomm
Colombia	ED	PARTLY FREE	24		✓	✓	✓			NEC
Czech Republic	LD		53	✓		✓	✓			
Denmark	LD		42		✓	✓	✓	✓	✓	Avigilon, BrainChip, Cisco, Hikvision, Palantir
Ecuador	ED	PARTLY FREE	55		✓	✓	✓	✓	✓	CEIEC, Cisco, Huawei
Egypt	EA	NOT FREE	51	✓		✓	✓	✓	✓	Honeywell, Huawei
France	LD	FREE	5		✓	✓	✓	✓	✓	Hikvision, Huawei, Palantir, Teleste, Thales, ZTE
Georgia	ED	FREE	100	✓		✓	✓			NEC
Germany	LD	FREE	8		✓	✓	✓	✓	✓	Cisco, Huawei, Palantir
Ghana	ED		110		✓			✓		Huawei
Hong Kong	ED					✓		✓		Bosch, Huawei

Appendix 1

AIGS Index Continued

CA	Closed Autocracy
EA	Electoral Autocracy/Competitive Autocracy
ED	Electoral Democracy/Illiberal Democracy
LD	Liberal Democracy

Country	Regime Type	"Freedom on the Net 2018" Status	Military Spending Ranking (2018)	BRI Country?	Smart/ Safe City?	Facial Recognition?	Smart Policing?	Chinese Tech?	U.S. Tech?	Key Companies
India	ED	PARTLY FREE	4		✓	✓	✓	✓	✓	ADRIN, Hikvision, IBM, Infinova, Microsoft, NEC
Indonesia	ED	PARTLY FREE	26	✓	✓	✓	✓	✓	✓	Huawei, NEC, PT Industri Telekomunikasi Indonesia
Iran	EA	NOT FREE	18	✓		✓	✓	✓		Hikvision
Iraq	EA		32	✓	✓	✓		✓		Huawei
Israel	ED		17	✓	✓	✓	✓		✓	AnyVision, BriefCam, Elbit, IBM, NICE, Verint
Italy	LD	FREE	11	✓	✓			✓		Huawei
Ivory Coast	ED		82		✓			✓		Huawei
Japan	LD	FREE	9		✓	✓	✓	✓		Hikvision, NEC
Kazakhstan	EA	NOT FREE	64	✓	✓	✓	✓	✓		Analytical Business Solutions, Huawei, Speech Technology Center
Kenya	EA	PARTLY FREE	69	✓	✓	✓	✓	✓		Huawei, NEC, Safaricom
Kyrgyzstan	EA	PARTLY FREE	118	✓	✓	✓	✓	✓		Huawei
Laos	CA			✓	✓		✓	✓		Huawei
Lebanon	EA	PARTLY FREE	52	✓	✓		✓		✓	Crestron, Guardia
Malaysia	ED	PARTLY FREE	49	✓	✓	✓	✓	✓		Huawei, NEC, Yitu
Malta	LD		128		✓	✓	✓	✓		Huawei
Mauritius	LD		141	✓	✓		✓	✓		Huawei
Mexico	ED	PARTLY FREE	31		✓	✓	✓	✓	✓	Cisco, Dahua, Infinova, Telmex, Thales
Mongolia	ED		122	✓		✓		✓		Dahua, SenseTime
Morocco	ED	PARTLY FREE	47	✓	✓	✓		✓		BAE, Huawei
Namibia	ED		89			✓	✓			Otesa
Netherlands	LD		21		✓	✓	✓	✓		Huawei, IDEMIA
New Zealand	LD		56	✓		✓	✓		✓	Palantir

Appendix 1

AIGS Index Continued

CA Closed Autocracy
EA Electoral Autocracy/Competitive Autocracy
ED Electoral Democracy/Illiberal Democracy
LD Liberal Democracy

Country	Regime Type	"Freedom on the Net 2018" Status	Military Spending Ranking (2018)	BRI Country?	Smart/ Safe City?	Facial Recognition?	Smart Policing?	Chinese Tech?	U.S. Tech?	Key Companies
Nigeria	EA	PARTLY FREE	57				✓	✓		Huawei
Oman	CA		30	✓	✓	✓		✓		BAE, Huawei, Idemia
Pakistan	EA	NOT FREE	20	✓	✓	✓	✓	✓		Huawei
Panama	ED			✓	✓	✓	✓	✓	✓	FaceFirst, Huawei, Infinova
Philippines	ED	PARTLY FREE	46	✓	✓	✓	✓	✓	✓	Boeing, CITCC, IBM, Huawei
Qatar	CA			✓	✓	✓	✓			BAE, Orange
Romania	ED		40	✓	✓			✓	✓	Cisco, Telekom Romania, ZTE
Russia	EA	NOT FREE	6	✓	✓	✓	✓	✓	✓	Analytical Business Solutions, Cisco, Huawei, NtechLab, Speech Technology Center
Rwanda	EA	PARTLY FREE	119	✓	✓			✓		Huawei
Saudi Arabia	CA	NOT FREE	3	✓	✓	✓	✓	✓	✓	Briefcam, Gatekeeper, Hikvision, Huawei, Hugslock, IBM, NEC
Serbia	ED		73	✓	✓	✓		✓		Huawei
Singapore	ED	PARTLY FREE	22	✓	✓	✓	✓	✓	✓	Accenture, AGT, Airbus, Dassault, Huawei, NEC, Tascent, Yitu
South Africa	ED	FREE	48	✓	✓	✓	✓	✓		Huawei
South Korea	LD	FREE	10	✓	✓	✓	✓		✓	Axis, IBM, Korea Telecom, LG Uplus, SK Telecom
Spain	LD		16		✓	✓	✓	✓	✓	Herta, Huawei, IBM, SICE
Switzerland	LD		38		✓	✓				Ekin
Taiwan	LD		23			✓				Gorilla, Lilin, NEC
Tajikistan	CA			✓	✓	✓		✓		Huawei
Thailand	EA	NOT FREE	29	✓	✓	✓		✓		Huawei, Megvii, Panasonic, ZTE
Turkey	EA	PARTLY FREE	15	✓		✓	✓	✓	✓	Avigilon, Dahua, Infinova, HAVESLAN, Infinova
Uganda	EA	PARTLY FREE	94		✓	✓		✓		Huawei

Appendix 1

AIGS Index Continued

CA Closed Autocracy
EA Electoral Autocracy/Competitive Autocracy
ED Electoral Democracy/Illiberal Democracy
LD Liberal Democracy

Country	Regime Type	"Freedom on the Net 2018" Status	Military Spending Ranking (2018)	BRI Country?	Smart/ Safe City?	Facial Recognition?	Smart Policing?	Chinese Tech?	U.S. Tech?	Key Companies
Ukraine	ED	PARTLY FREE	39	✓	✓	✓		✓	✓	Hikvision, Huawei, Microsoft
United Arab Emirates	CA	NOT FREE		✓	✓	✓	✓	✓	✓	BAE, BriefCam, Hikvision, Huawei, IBM, NEC
United Kingdom	LD	FREE	7		✓	✓	✓	✓	✓	Hikvision, NEC, Palantir
United States of America	LD	FREE	1		✓	✓	✓	✓	✓	Mult; Amazon, Hikvision, IBM, Infinova, Palantir, PredPol, Pelco, Avigilon
Uruguay	LD		68		✓	✓	✓	✓	✓	Palantir, Herta, ZTE
Uzbekistan	CA	NOT FREE		✓	✓	✓		✓		Huawei, Infinova, Speech Technology Center
Venezuela	CA	NOT FREE		✓		✓		✓		CEIEC, Huawei, ZTE
Zambia	EA	PARTLY FREE	98			✓		✓		Hikvision, Huawei, ZTE
Zimbabwe	EA	PARTLY FREE	91			✓	✓	✓		CloudWalk, Hikvision, Huawei

Source Notes:
Aggregate Regime Score: Comprised of evenly weighted average of country scores from Freedom in the World 2019, https://freedomhouse.org/report/countries-world-freedom-2019; the EIU Democracy Index 2018, https://www.eiu.com/topic/democracy-index; and the V-Dem Dataset version 9, Electoral Democracy Index, https://www.v-dem.net/en/data/data-version-9/.

Regime Type: The AIGS Index uses a four-part regime category typology established by V-Dem and Regimes of the World: closed autocracies, electoral autocracies, electoral democracies, and liberal democracies. Countries with an average score less than 2.5 are labeled closed autocracies. Countries with an average score between 2.5 and 4.9 are labeled electoral autocracies. Countries with an average score less than 8 are labeled electoral democracies. Countries with an average score of 8 or higher are labeled liberal democracies. See Anna Lührmann, Marcus Tannenberg, and Staffan I. Lindberg, "Regimes of the World (RoW): Opening New Avenues for the Comparative Study of Political Regimes," Politics & Governance 6, no. 1 (2018).

"Freedom on the Net 2018" data can be accessed at https://freedomhouse.org/report/freedom-net/freedom-net-2018.

Military expenditure data compiled by the Stockholm International Peace Research Institute and can be accessed at https://www.sipri.org/databases/milex.

Data on Belt and Road Initiative participating countries compiled from Dan Kliman and Abigail Grace's report, "Power Play: Addressing China's Belt and Road Strategy," Center for a New American Security, 2018, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Power-Play-Addressing-Chinas-Belt-and-Road-Strategy.pdf?mtime=20180920093003, as well as from open source reporting.

Data for China's overseas direct investment compiled by the Economist Intelligence Unit, "China Going Global Investment Index 2017," http://pages.eiu.com/rs/753-RIQ-438/images/ODI_in_China_2017_English.pdf.

Appendix 2

Taxonomy of Digital Repression

Techniques of Digital Repression

Surveillance	Censorship	Disinformation	Cyber Attacks & Hacking	Internet Shutdowns	Targeted Arrests & Violence
AI surveillance (facial recognition systems, intelligent video surveillance, smart policing, smart cities/safe cities) ***Communications surveillance*** (internet/social media monitoring, mobile phone tapping/SIM registration, location monitoring, intrusion spyware, packet inspection, network interception, cable tapping, telecom surveillance) ***Surveillance laws*** (intelligence/national security laws, data disclosure, data retention, data localization)	***Political & social content blocked/ filtered; use of friction & flooding*** ***Social media/ICT apps blocked*** ***Content removal*** ***Censorship laws/ directives:*** Religion/blasphemy Cyber crime False news Political/hate speech Lèse-majesté Security/terrorism Sedition Copyright infringement Defamation/libel Indecency/anti-LGBT ***Financial targeting of groups***	Government/ pro-government outlets peddle disinformation, false content Cyber trolling, social media manipulation/ harassment by pro-government actors (astroturfing, bots, sockpuppets, impersonation) Election manipulation (for example, data exploitation)	State-sponsored technical attacks which manipulate software, data, computer systems, or networks to degrade operational capabilities or collect information ***Categories:*** Attacks harming operational capacity Intrusion and surveillance attacks ***Illustrative Tools:*** Vandalism Distributed denial of service Man-in-the-middle Phishing Advanced persistent threat Spoofing Border Gateway Protocol	***Internet or electronic communications disrupted*** Total internet shutdowns Partial shutdowns (restricted website/ social media access, blackouts, slowdowns, throttling) ***Infrastructure restrictions*** (internet firewall; closed ICT infrastructure)	ICT user charged, arrested, imprisoned, or in prolonged detention for political/social content ICT user physically attacked or killed

About the Author

Steven Feldstein is a nonresident fellow in Carnegie's Democracy, Conflict, and Governance Program, where he focuses on the intersection of technology, democracy, and human rights; U.S. foreign policy; and Africa policy. He is also an associate professor and the holder of the Frank and Bethine Church Chair of Public Affairs at Boise State University. He served as a deputy assistant secretary for democracy, human rights, and labor in the U.S. Department of State from 2014 to 2017. He is writing a book examining global trends of digital repression.

Acknowledgments

Special thanks to Luke Lamey, undergraduate at Georgetown University, for research assistance in compiling references for the AI Global Surveillance Index. Many thanks also go to Jon Bateman and Thomas Carothers (Carnegie Endowment for International Peace), Adrian Shabhaz (Freedom House), Brian Wampler (Boise State University), and Nick Wright (Intelligent Biology, Georgetown University) for generously giving their time to read through prior drafts of this paper and to offer invaluable feedback and advice.

Notes

1 The index uses a four-part regime category typology established by V-Dem and Regimes of the World: closed autocracies, electoral autocracies, electoral democracies, and liberal democracies. As the authors describe it, "In closed autocracies, the chief executive is either not subjected to elections or there is no meaningful, de-facto competition in elections. Electoral autocracies hold de-facto multiparty elections for the chief executive, but they fall short of democratic standards due to significant irregularities, limitations on party competition or other violations of Dahl's institutional requisites for democracies. To be counted as electoral democracies, countries not only have to hold defacto free and fair and multiparty elections, but also . . . achieve a sufficient level of institutional guarantees of democracy such as freedom of association, suffrage, clean elections, an elected executive, and freedom of expression. A liberal democracy is, in addition, characterized by its having effective legislative and judicial oversight of the executive as well as protection of individual liberties and the rule of law." Anna Lührmann, Marcus Tannenberg, and Staffan I. Lindberg, "Regimes of the World (RoW): Opening New Avenues for the Comparative Study of Political Regimes," *Politics & Governance* 6, no. 1 (2018).

2 Information from the Stockholm International Peace Research Institute (SIPRI), SIPRI Military Expenditure Database, 2019, https://www.sipri.org/databases/milex.

3 "Freedom on the Net 2018: The Rise of Digital Authoritarianism," Freedom House, October 30, 2018. https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

4 In contrast to V-Dem, the AIGS Index does not evaluate the Palestinian Territories (West Bank, Gaza) and Zanzibar due to inconsistent treatment by external sources. See Michael Coppedge, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, David Altman, Michael Bernhard, et al, "V-Dem Country-Year Dataset 2019," Varieties of Democracy (V-Dem) Project, 2019, https://doi.org/10.23696/vdemcy19.

5 Nils J. Nilsson, *The Quest for Artificial Intelligence* (United States: Cambridge University Press, 2009), 4.

6 "Preparing for the Future of Artificial Intelligence," whitehouse.gov, October 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

7 Ibid.

8 As described in the executive summary, in contrast to V-Dem, the AIGS Index does not evaluate the Palestinian Territories (West Bank, Gaza) and Zanzibar due to inconsistent treatment by external sources. "V-Dem Country-Year Dataset 2019," 2019.

9 "Freedom on the Net 2018: The Rise of Digital Authoritarianism," October 30, 2018, 9.

10 "Digital 2019: Internet Trends in Q3 2019," DataReportal—Global Digital Insights, July 19, 2019. https://datareportal.com/reports/digital-2019-internet-trends-in-q3.

11 Kim Hart, "Baltimore Wrestles With Aerial Surveillance," Axios, July 31, 2019, https://www.axios.com/baltimore-wrestles-with-aerial-surveillance-to-reduce-crime-2d973591-0b33-4e25-94a7-c3f553dc2934.html.

12 Kevin Rector and Alison Knezevich, "Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates," *Baltimore Sun*, October 18, 2016, https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html.

13 "Persistent Surveillance's Cynical Attempt to Profit Off Baltimore's Trauma," ACLU of Maryland, June 8, 2018, https://www.aclu-md.org/en/press-releases/persistent-surveillances-cynical-attempt-profit-baltimores-trauma.

14 Olivia Solon, "'Surveillance Society': Has Technology at the US-Mexico Border Gone Too Far?," *Guardian*, June 13, 2018, https://www.theguardian.com/technology/2018/jun/13/mexico-us-border-wall-surveillance-artificial-intelligence-technology.

[15] Alvaro Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets," IBEI Working Paper, 2017, https://www.ibei.org/surveillance-smart-technologies-and-the-development-of-safe-city-solutions-the-case-of-chinese-ict-firms-and-their-international-expansion-to-emerging-markets_112561.pdf.

[16] Theodore Terschlusen, "Valencienne: Demain Les Caméras de Vidéosurveillance Seront Intelligentes Et…Chinoises," September 2, 2017, https://webcache.googleusercontent.com/search?q=cache:FS-IyIma564J:www.lavoixdunord.fr/116566/article/2017-02-09/demain-les-cameras-de-videosurveillance-seront-intelligentes-et-chinoises+&cd=1&hl=en&ct=clnk&gl=us.

[17] SIPRI Military Expenditure Database, 2019.

[18] "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue," A/HRC/23/40, April 17, 2013, https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[19] "The Right to Privacy in the Digital Age," Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, June 30, 2014, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf. See also article 12 of the Universal Declaration of Human Rights.

[20] "Surveillance and Human Rights, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/HRC/41/35, May 28, 2019, https://undocs.org/A/HRC/41/35.

[21] "Necessary and Proportionate," Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, March 4, 2016. https://necessaryandproportionate.org/principles.

[22] "The Right to Privacy in the Digital Age," A/HRC/27/37.

[23] "Surveillance and Human Rights," A/HRC/41/35.

[24] Steven Feldstein, "Can a U.N. Report Help Rein in Expansive and Abusive Digital Surveillance?," *World Politics Review*, July 9, 2019, https://www.worldpoliticsreview.com/articles/28016/can-a-u-n-report-help-rein-in-expansive-and-abusive-digital-surveillance.

[25] "The Right to Privacy in the Digital Age," A/HRC/27/37.

[26] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue," A/HRC/23/40.

[27] Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," *Journal of Democracy* 30, no. 1 (2019): 42.

[28] Nicholas Wright notes: "People will know that the omnipresent monitoring of their physical and digital activities will be used to predict undesired behavior, even actions they are merely contemplating. . . . In order to prevent the system from making negative predictions, many people will begin to mimic the behaviors of a "responsible" member of society. These may be as subtle as how long one's eyes look at different elements on a phone screen. This will improve social control not only by forcing people to act in certain ways, but also by changing the way they think." Nicholas Wright, "How Artificial Intelligence Will Reshape the Global Order," *Foreign Affairs*, July 10, 2018, https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

[29] See Jeffrey Ding, "Deciphering China's AI Dream," Future of Humanity Institute, University of Oxford, 2018, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.

[30] See for example: "China's Digital Authoritarianism: Surveillance, Influence, and Political Control," U.S. House of Representatives, Permanent Select Committee on Intelligence, committee hearing, May 16, 2019, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=109462; Robert Morgus and Justin Sherman, "Authoritarians Are Exporting Surveillance Tech, And With It Their Vision for the

Internet," Council on Foreign Relations, December 5, 2018, https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet; "Freedom on the Net 2018: The Rise of Digital Authoritarianism," October 30, 2018; and Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

31 "Yanbu: A Smart Industrial Oil Kingdom City — Huawei Publications," Huawei, 2019, https://e.huawei.com/us/publications/global/ict_insights/201708310903/manufacturing/201712061133 ; Sebastian Moss, "Google Cloud Continues to Grow, Is Coming to Saudi Arabia," Data Centre Dynamics, April 24, 2018, https://www.datacenterdynamics.com/news/google-cloud-continues-to-grow-is-coming-to-saudi-arabia/; Rob Evans, "BAE 'Secretly Sold Mass Surveillance Technology to Repressive Regimes,'" *Guardian*, June 14, 2017, https://www.theguardian.com/business/2017/jun/15/bae-mass-surveillance-technology-repressive-regimes; Triska Hamid, "NEC Profits from Middle East Cyber Fears," The National, December 10, 2013, https://www.thenational.ae/business/nec-profits-from-middle-east-cyber-fears-1.267420; and Alaa Shahine, Erik Schatzker, Vivian Nereim, and Glen Carey, "Saudis Are Talking to Amazon, Alibaba About New City, Prince Says," *Bloomberg*, October 26, 2017, https://www.bloomberg.com/news/articles/2017-10-26/saudis-are-talking-to-amazon-alibaba-over-new-city-prince-says.

32 Korkit Danchaivichit (deputy secretary general of the National Telecommunications and Broadcasting Commission), interview with the author, May 17, 2019.

33 Joe Parkinson, Nicholas Bariyo and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 14, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

34 "Uganda's Cash-Strapped Cops Spend $126 Million on CCTV from Huawei," Reuters, August 16, 2019, https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF.

35 Danielle Cave Thomas, Samantha Hoffman, Alex Joske, and Fergus Ryan, Elise, "Mapping China's Tech Giants," Australian Strategic Policy Institute, Issues Paper, Report No. 15/2019, https://www.aspi.org.au/report/mapping-chinas-tech-giants.

36 "Building a Safe Mauritius, the Inspiration for Heaven," Huawei, 2019, https://e.huawei.com/topic/leading-new-ict-en/mauritius-safecity-case.html.

37 Anna Fifield, "Bloodthirsty Like a Wolf: Inside the Military Style Discipline at China's Tech Titan Huawei," *Washington Post*, December 13, 2018, https://www.washingtonpost.com/world/asia_pacific/bloodthirsty-like-a-wolf-inside-the-military-style-discipline-at-chinas-tech-titan-huawei/2018/12/12/76055116-fd85-11e8-a17e-162b712e8fc2_story.html?noredirect=on&utm_term=.fca5427820cf.

38 The EU's former top trade official, Karel De Gucht, is on record observing: "They [Huawei] get subsidies. If you have a line of a couple of tens of billions with the bank that you can use at your discretion this is a huge subsidy, no?" Shawn Donnan and Christian Oliver, "EU Commissioner Attacks China's Telecoms Subsidies," *Financial Times*, March 27, 2014, https://www.ft.com/content/d6d0bcc6-b5cb-11e3-b40e-00144feabdc0. Likewise, a 2012 U.S. congressional report from the House Intelligence Committee noted that Huawei reaps the "benefit of billions of dollars in Chinese government financing," and that both Huawei and ZTE "provide a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants into critical telecommunications components and systems." "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," U.S. House of Representatives, Permanent Select Committee on Intelligence,

October 8, 2012, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf, 3.

[39] Max Chafkin and Joshua Brustein, "Why America Is So Scared of China's Biggest Tech Company," *Bloomberg Businessweek*, March 23, 2018, https://www.bloomberg.com/news/features/2018-03-22/why-america-is-so-scared-of-china-s-biggest-tech-company.

[40] Ibid.

[41] Zhang Lin, "Chinese Communist Party Needs to Curtail Its Presence in Private Businesses," *South China Morning Post*, November 25, 2018, https://www.scmp.com/economy/china-economy/article/2174811/chinese-communist-party-needs-curtail-its-presence-private.

[42] Arjun Kharpal, "Huawei CEO: No Matter My Communist Party Ties, I'll 'Definitely' Refuse If Beijing Wants Our Customers' Data," CNBC, January 15, 2019, https://www.cnbc.com/2019/01/15/huawei-ceo-we-would-refuse-a-chinese-government-request-for-user-data.html.

[43] Paul Mozur, "China's Internet Controls Will Get Stricter, to Dismay of Foreign Business," *New York Times*, November 7, 2016, https://www.nytimes.com/2016/11/08/business/international/china-cyber-security-regulations.html.

[44] Christopher Balding and Donald C. Clarke, "Who Owns Huawei?" SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, April 17, 2019, https://papers.ssrn.com/abstract=3372669.

[45] Author interview with an official from Thailand's Ministry of Interior, May 14, 2019.

[46] Somkiat Tangkitvanich (president, Thailand Development Research Institute), interview with the author, May 14, 2019.

[47] Christian Davenport, "State Repression and Political Order," *Annual Review of Political Science* 10 (2007): 2.

[48] "Smart Cities," World Bank, January 8, 2015, https://www.worldbank.org/en/topic/digitaldevelopment/brief/smart-cities.

[49] "Smart Cities: Utopian Vision, Dystopian Reality," Privacy International, October 2017, http://www.privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality.

[50] "Huawei Smart City White Paper," Huawei Enterprise, 2016, https://e.huawei.com/en/material/onLineView?MaterialID=9b0000e57fa94a2dbc0e43f5817ca767.

[51] Ibid.

[52] "The Road to Collaborative Public Safety," Huawei, 2017, http://e-file.huawei.com/~/media/EBG/Download_Files/Publications/en/Safe%20City%20Extra.pdf.

[53] "Three Rules When Using AI to Add Value to Your IoT Smart Cities," Gartner, January 29, 2018, https://www.gartner.com/doc/reprints?id=1-4XYENKG&ct=180501&st=sb.

[54] Bojan Stojkovski, "Big Brother Comes to Belgrade," *Foreign Policy*, June 18, 2019, accessed July 29, 2019, https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/.

[55] "Huawei Safe City Solution: Safeguards Serbia," Huawei Enterprise, August 23, 2018, http://archive.li/pZ9HO.

[56] Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," 40.

[57] "Video Surveillance as the Foundation of 'Safe City' in Kenya," Huawei, 2019, https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya. See also Victor Kapiyo and Grace Githaiga, "Kenya, Communications Surveillance in the Digital Age," Global Information Society Watch," 2014, https://www.giswatch.org/en/country-report/communications-surveillance/kenya.

[58] Drew Harrell, "FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches," *Washington Post*, July 7, 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[59] Rowland Manthorpe and Alexander J Martin, "81% of 'Suspects' Flagged by Met's Police Facial Recognition Technology Innocent, Independent Report Says," Sky News, July 4, 2019, https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941.

[60] Charlie Warzel, "A Major Police Body Cam Company Just Banned Facial Recognition," *New York Times*, June 27, 2019, https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html.

[61] "NIST Evaluation Shows Advance in Face Recognition Software's Capabilities," U.S. National Institute for Standards and Technology, November 30, 2018, https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

[62] Steve Lohr, "Facial Recognition Is Accurate, If You're a White Guy," *New York Times*, February 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[63] Paul Mozur, "In Hong Kong Protests, Faces Become Weapons," *New York Times*, July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

[64] Randy Rieland, "Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?" *Smithsonian*, March 5, 2018. https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/.

[65] Caroline Haskins, "Revealed: This Is Palantir's Top-Secret User Manual for Cops," *Vice*, July 12, 2019, https://www.vice.com/en_us/article/9kx4z8/revealed-this-is-palantirs-top-secret-user-manual-for-cops.

[66] "The Three Pillars of Predictive Policing," PredPol, 2018, https://www.predpol.com/law-enforcement/.

[67] "China: Big Data Fuels Crackdown in Minority Region," Human Rights Watch, February 26, 2018, https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.

[68] Cate Cadell, "From Laboratory in Far West, China's Surveillance State Spreads," Reuters, August 14, 2018, https://www.reuters.com/article/us-china-monitoring-insight-idUSKBN1KZ0R3; "China: Minority Region Collects DNA from Millions," Human Rights Watch, December 13, 2017, https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.

[69] Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," 45.

[70] Jeffrey Ding, "ChinAI #59: Is Winter Coming for Hikvision?," accessed July 28, 2019, https://chinai.substack.com/p/chinai-59-is-winter-coming-for-hikvision.

[71] For an in-depth look at the AI machine learning value chain, including an incisive examination of data storage modalities, see: Charlotte Stanton et al., "What the Machine Learning Value Chain Means for Geopolitics," Carnegie Endowment for International Peace, August 5, 2019, https://carnegieendowment.org/files/7-1-19_Stanton_etal_Machine_Learning.pdf.

[72] "Accenture Automated Border Clearance Solutions," Accenture, 2019, https://www.accenture.com/us-en/service-border-management-automated-border-clearance-summary.

[73] "EGate Solutions: Automated Border Control (ABC)," Gemalto, April 12, 2019, https://www.gemalto.com/govt/coesys/eborder-abc.

[74] "IBorderCtrl: The Project," iBorderCtrl, 2016, https://www.iborderctrl.eu/The-project.

[75] Lisa Feldman Barrett, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez, and Seth D. Pollak, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements," *Psychological Science in the Public Interest*, July 17, 2019, https://doi.org/10.1177/1529100619832930. See also Lucien Begault, "Automated Technologies and the Future of Fortress Europe," Amnesty International, March 28, 2019, https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/.

[76] Patricia Moloney Figliola and Eric A Fischer, "Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management," Congressional Research Service, January 20, 2015, https://fas.org/sgp/crs/misc/R42887.pdf

[77] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, September 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[78] Esat Dedezade, "Iceland to Become the First 'Cloud-First-Nation,'" Microsoft News Centre Europe, September 19, 2018, https://news.microsoft.com/europe/features/iceland-to-become-the-first-cloud-first-nation/.

[79] Mehul Srivastava and Tim Bradshaw, "Israeli Group's Spyware 'Offers Keys to Big Tech's Cloud'," *Financial Times*, July 19, 2019, https://www.ft.com/content/95b91412-a946-11e9-b6ee-3cdf3174eb89.

[80] "Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence," Report of the 2015-2016 Study Panel, Stanford University, September 2016, https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.

[81] Ibid.

[82] Jonathan L. Zittrain, Matthew G. Olsen, David O'Brien, and Bruce Schneier, "Don't Panic: Making Progress on the "Going Dark" Debate." Berkman Center Research Publication 2016-1, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

[83] Matt Day, Giles Turner, and Natalia Drozdiak, "Amazon Workers Are Listening to What You Tell Alexa," *Bloomberg*, April 10, 2019, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[84] Greg Bensinger, "Google Employs Humans to Listen to Some Voice-Assistant Recordings," *Washington Post*, July 11, 2019, https://www.washingtonpost.com/technology/2019/07/11/google-employs-humans-listen-some-voice-assistant-recordings/.

[85] Andy Greenberg, "This Tesla Mod Turns a Model S Into a Mobile 'Surveillance Station,'" *Wired*, August 9, 2019, https://www.wired.com/story/tesla-surveillance-detection-scout/.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org

Algorithms and Justice

Ethics and Governance of Artificial Intelligence Initiative

Government institutions around the globe are beginning to explore decision automation in a variety of contexts, from determining eligibility for services; to evaluating where to deploy health inspectors and law enforcement personnel; to defining boundaries around voting districts. Use cases for technologies that incorporate AI or machine learning will expand as governments and companies amass larger quantities of data and analytical tools become more powerful.

The criminal justice system offers valuable insight into government use of algorithmic technology. With fallible judges, juries, and lawyers, that system has been rightly criticized for inconsistency and for perpetuating practices that disproportionately harm marginalized groups. Support for reexamination of detention practices has grown in recent years, as reformers and state institutions alike seek to control costs, manage overcrowded prison systems, and address disparate impacts of incarceration.

To the extent they inject clarity and precision into bail, parole, and sentencing decisions, algorithmic technologies may minimize harms that are the products of human judgment. Conversely, the use of technology to determine whose liberty is deprived and on what terms raises significant concerns about transparency and interpretability. We must consider both legal and ethical issues and engage in rigorous testing and evaluation to ensure adoption of algorithmic tools satisfies notions of procedural and substantive fairness and does not reinforce institutional biases.

As its name suggests, the criminal justice system is not a unified construct but a series of interconnected processes, with multiple entry points and stages of evaluation. Technology may help to balance among goals of deterrence, incapacitation, rehabilitation, restitution, and retribution, shedding light on what causes criminal behavior and appropriate responses thereto. Each stage in the development, procurement, deployment, and assessment of each technological tool raises distinct and essential questions that demand a multiplicity of approaches.

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

23 Everett St., 2nd Floor
Cambridge, MA 02138

cyber.harvard.edu
hello@cyber.harvard.edu
@BKCHarvard
617.495.7547

The Algorithms and Justice project: (a) explores ways in which government institutions incorporate artificial intelligence, algorithms, and machine learning technologies into their decisionmaking; and (b) in collaboration with our colleagues working on Global Governance issues, examines ways in which development and deployment of these technologies by both public and private actors impacts the rights of individuals and efforts to achieve social justice. Our aim is to help companies that create such tools, state actors that procure and deploy them, and citizens they impact to understand how those tools work. We seek to ensure that algorithmic applications are developed and used with an eye toward improving fairness and efficacy without sacrificing values of accountability and transparency.

In undertaking this work, the **Berkman Klein Center** will draw on its rich history of delving into hard law and policy questions via research and engagement with government actors and innovators. The **MIT Media Lab** will draw on its rigorous application of research methods, technical expertise, and outside-the-box thinking.

Challenges that we seek to address in our work include:

› **Transparency**: The law traditionally places great importance on transparency in the workings of government and—in particular—in the administration of the justice system. Development processes and methodologies can be opaque, and jurisdictions do not always provide access to data that allows for oversight of technology-enabled decisions. For this reason, we are building a database of the most common risk assessment tools used in the United States, to illuminate the methodologies and limitations of such tools.

› **Bias**: In the United States and elsewhere, historically-marginalized groups are often over-represented in incarcerated populations. Algorithmic systems trained on historical data must therefore confront inherent biases. Existing assessment tools approach the legacy of unequal outcomes in different ways. But little is known about the effectiveness of their methods, and there exists considerable debate about the extent to which these factors (and their proxies) can be isolated.

› **Due process**: Use of technology in the criminal justice system has the potential to upend centuries-old conceptions of due process and force debates about adapting norms to suit the digital age. The outcome of those debates will hinge on whether new challenges are analogous to past ones (from which we can learn), or whether they represent an existential crisis for the judicial system (demanding a reimagining of criminal liability and punishment). Addressing these issues requires an interdisciplinary approach, translating concepts of justice and fairness between lawyers and policymakers (on the one hand) and technologists (on the other). Importantly, by partnering with local communities, we are working to demonstrate that the judicious and timely application of technology in can actually improve social service deliver, reduce interactions with the judicial system, and better advance the core motivations of the justice system as a whole.

› **Competing priorities**: Undeniable tensions exist among commercial interests of those that build and sell technology; cost-management interests of government officers that procure tech tools; and societal interests of citizens seeking to preserve norms and values around fairness, justice, and accountability. This is why it is critical that we are working closely with state attorneys general, and court administrators to develop resources to help manages these competing priorities.

› **Interpretability and Dynamic Adaptation**: Most government decisions (including decisions about incarceration) are accompanied by legal analyses and justifications. But algorithms may not offer explanations that laypersons can understand, and the dynamic nature of machine learning might yield different results in one case today and a similar case tomorrow. It is vital that we ensure results are interpretable and that any inconsistencies can be explained. To advance this, we are supporting an interdisciplinary group of lawyers and computer scientists who are working on a framework to help policymakers understand the advantages and limitations of algorithmic explanations, so that policies can be grounded in technically feasible approaches.

Pillars of Impact

In building solutions that address these challenges, our institutions are making a series of investments, most significantly in:

1. Launching a **database of risk assessment tools used across criminal justice contexts**, including information about where and how they are used; development and validation practices; and legal, legislative, and/or media responses to their use.

2. Leading opportunities for **government officials at federal, state, and local levels** to engage with academic, civil society, and private sector constituents to tackle emerging regulatory and enforcement questions related to AI and algorithms.

3. Work with jurisdictions to develop **best practices around the procurement and deployment of criminal justice related risk assessment tools** to govern their adoption and create frameworks for assessing impact.

About the Ethics and Governance of Artificial Intelligence Initiative

The rapidly growing capabilities and increasing presence of AI-based systems in our lives raise pressing questions about the impact, governance, ethics, and accountability of these technologies around the world. How can we narrow the knowledge gap between AI "experts" and the variety of people who use, interact with, and are impacted by these technologies? How do we harness the potential of AI systems while ensuring that they do not exacerbate existing inequalities and biases, or even create new ones? At the Berkman Klein Center, a wide range of research projects – including the one outlined above – community members, programs, and perspectives seek to address the big questions related to the ethics and governance of AI under the Ethics and Governance of AI Initiative, launched in 2017.

USING ARTIFICIAL INTELLIGENCE TO ADDRESS CRIMINAL JUSTICE NEEDS

BY **CHRISTOPHER RIGANO**

NIJ is committed to realizing the full potential of artificial intelligence to promote public safety and reduce crime.

"Intelligent machines" have long been the subject of science fiction. However, we now live in an era in which artificial intelligence (AI) is a reality, and it is having very real and deep impacts on our daily lives. From phones to cars to finances and medical care, AI is shifting the way we live.

AI applications can be found in many aspects of our lives, from agriculture to industry, commun-ications, education, finance, government, service, manufacturing, medicine, and transportation. Even public safety and criminal justice are benefiting from AI. For example, traffic safety systems identify violations and enforce the rules of the road, and crime forecasts allow for more efficient allocation of policing resources. AI is also helping to identify the potential for an individual under criminal justice supervision to reoffend.[1]

Research supported by NIJ is helping to lead the way in applying AI to address criminal justice needs, such as identifying individuals and their actions in videos relating to criminal activity or public safety, DNA analysis, gunshot detection, and crime forecasting.

What Is Artificial Intelligence?

AI is a rapidly advancing field of computer science. In the mid-1950s, John McCarthy, who has been credited as the father of AI, defined it as "the science and engineering of making intelligent machines" (see sidebar, "A Brief History of Artificial Intelligence").[2] Conceptually, AI is the ability of a machine to perceive and respond to its environment independently and perform tasks that would typically require human intelligence and decision-making processes, but without direct human intervention.

Artificial intelligence has the potential to be a permanent part of our criminal justice ecosystem, providing investigative assistance and allowing criminal justice professionals to better maintain public safety.

One facet of human intelligence is the ability to learn from experience. Machine learning is an application of AI that mimics this ability and enables machines and their software to learn from experience.[3] Particularly important from the criminal justice perspective is pattern recognition. Humans are efficient at recognizing patterns and, through experience, we learn to differentiate objects, people, complex human emotions, information, and conditions on a daily basis. AI seeks to replicate this human capability in software algorithms and computer hardware. For example, self-learning algorithms use data sets to understand how to identify people based on their images, complete intricate computational and robotics tasks, understand purchasing habits and patterns online, detect medical conditions from complex radiological scans, and make stock market predictions.

Applications for Criminal Justice and Public Safety

AI is being researched as a public safety resource in numerous ways. One particular AI application — facial recognition — can be found everywhere in both the public and the private sectors (see sidebar, "The National Artificial Intelligence Research and Development Strategic Plan").[4] Intelligence analysts, for example, often rely on facial images to help establish an individual's identity and whereabouts. Examining the huge volume of possibly relevant images and videos in an accurate and timely manner is a time-consuming, painstaking task, with the potential for human error due to fatigue and other factors. Unlike humans, machines do not tire. Through initiatives such as the Intelligence Advanced Research Projects Activity's Janus computer-vision project, analysts are performing trials on the use of algorithms that can learn how to distinguish one person from another using facial features in the same manner as a human analyst.[5]

The U.S. Department of Transportation is also looking to increase public safety through researching, developing, and testing automatic traffic accident detection based on video to help maintain safe and efficient commuter traffic over various locations and weather, lighting, and traffic conditions.[6] AI algorithms are being used in medicine to interpret radiological images, which could have important implications for the criminal justice and medical examiner communities when establishing cause and manner of death.[7] AI algorithms have also been explored in various disciplines in forensic science, including DNA analysis.[8]

AI is also quickly becoming an important technology in fraud detection.[9] Internet companies like PayPal stay ahead of fraud attempts by using volumes of data to continuously train their fraud detection algorithms to predict and recognize anomalous patterns and to learn to recognize new patterns.[10]

NIJ's Artificial Intelligence Research Portfolio

The AI research that NIJ supports falls primarily into four areas: public safety video and image analysis, DNA analysis, gunshot detection, and crime forecasting.

Public safety video and image analysis

Video and image analysis is used in the criminal justice and law enforcement communities to obtain information regarding people, objects, and actions to support criminal investigations. However, the analysis of video and image information is very labor-intensive, requiring a significant investment in personnel with subject matter expertise. Video and image analysis is

also prone to human error due to the sheer volume of information, the fast pace of changing technologies such as smartphones and operating systems, and a limited number of specialized personnel with the knowledge to process such information.

AI technologies provide the capacity to overcome such human errors and to function as experts. Traditional software algorithms that assist humans are limited to predetermined features such as eye shape, eye color, and distance between eyes for facial recognition or demographics information for pattern analysis. AI video and image algorithms not only learn complex tasks but also develop and determine their own independent complex facial recognition features/parameters to accomplish these tasks, beyond what humans may consider. These algorithms have the potential to match faces, identify weapons and other objects, and detect complex events such as accidents and crimes (in progress or after the fact).

In response to the needs of the criminal justice and law enforcement communities, NIJ has invested in several areas to improve the speed, quality, and specificity of data collection, imaging, and analysis and to improve contextual information.

For instance, to understand the potential benefits of AI in terms of speed, researchers at the University of Texas at Dallas, with funding from NIJ and in partnership with the FBI and the National Institute of Standards and Technology, are assessing facial identification by humans and examining methods for effectively comparing AI algorithms and expert facial examiners. Preliminary results show that when the researchers limit the recognition time to 30 seconds, AI-based facial-recognition algorithms developed in 2017 perform comparably to human facial examiners.[11] The implications of these findings are that AI-based algorithms can potentially be used as a "second pair of eyes" to increase the accuracy of expert human facial examiners and to triage data to increase productivity.

In addition, in response to the need for higher quality information and the ability to use lower quality images more effectively, Carnegie Mellon University is using NIJ funding to develop AI algorithms to improve detection, recognition, and identification. One particularly important aspect is the university's work on images in which an individual's face is captured at different angles or is partially to the side, and when the individual is looking away from the camera, obscured by masks or helmets, or blocked by lamp posts or lighting. The researchers are also working with low-quality facial image construction, including images with poor resolution and low ambient light levels, where the image quality makes facial matching difficult. NIJ's test and evaluation center is currently testing and evaluating these algorithms.[12]

Finally, to decipher a license plate (which could help identify a suspect or aid in an investigation) or identify a person in extremely low-quality images or video, researchers at Dartmouth College are using AI algorithms that systematically degrade high-quality images and compare them with low-quality ones to better recognize lower quality images and video. For example, clear images of numbers and letters are slowly degraded to emulate low-quality images. The degraded images are then expressed and catalogued as mathematical representations. These degraded mathematical representations can then be compared with low-quality license plate images to help identify the license plate.[13]

Also being explored is the notion of "scene understanding," or the ability to develop text that describes the relationship between objects (people, places, and things) in a series of images to provide context. For example, the text may be "Pistol being drawn by a person and discharging into a store window." The goal is to detect objects and activities that will help identify crimes in progress for live observation and intervention as well as to support investigations after the fact.[14] Scene understanding over multiple scenes can indicate potentially important events that law enforcement should view to confirm and follow. One group of researchers at the University of Central Florida, in partnership with the Orlando Police Department, is using NIJ funding to develop algorithms to identify objects in videos, such as people, cars, weapons, and buildings, without human intervention. They are also developing algorithms to

A Brief History of Artificial Intelligence

1950: Alan Turing publishes his paper on creating thinking machines.[1]

1956: John McCarthy presents his definition of artificial intelligence.[2]

1956-1974: Reason searches or means-to-end algorithms were first developed to "walk" simple decision paths and make decisions.[3] Such approaches provided the ability to solve complex mathematical expressions and process strings of words. The word processing is known as natural language processing. These approaches led to the ability to formulate logic and rules to interpret and formulate sentences and also marked the beginning of game theory, which was realized in basic computer games.[4]

1980-1987: Complex systems were developed using logic rules and reasoning algorithms that mimic human experts. This began the rise of expert systems, such as decision support tools that learned the "rules" of a specific knowledge domain like those that a physician would follow when performing a medical diagnosis.[5] Such systems were capable of complex reasoning but, unlike humans, they could not learn new rules to evolve and expand their decision-making.[6]

1993-2009: Biologically inspired software known as "neural networks" came on the scene. These networks mimic the way living things learn how to identify complex patterns and, in doing so, can complete complex tasks. Character recognition for license plate readers was one of the first applications.[7]

2010-present: Deep learning and big data are now in the limelight. Affordable graphical processing units from the gaming industry have enabled neural networks to be trained using big data.[8] Layering these networks mimics how humans learn to recognize and categorize simple patterns into complex patterns. This software is being applied in automated facial and object detection and recognition as well as medical image diagnostics, financial patterns, and governance regulations.[9] Projects such as Life Long Learning Machines, from the Defense Advanced Research Projects Agency, seek to further advance AI algorithms toward learning continuously in ways similar to those of humans.[10]

Notes

1. Alan Turing, "Computing Machinery and Intelligence," *Mind* 49 (1950): 433-460.

2. The Society for the Study of Artificial Intelligence and Simulation of Behaviour, "What is Artificial Intelligence."

3. Herbert A. Simon, *The Sciences of the Artificial* (Cambridge, MA: MIT Press, 1981).

4. Daniel Crevier, *AI: The Tumultuous Search for Artificial Intelligence* (New York: Basic Books, 1993), ISBN 0-465-02997-3.

5. Ibid.

6. Pamela McCorduck, *Machines Who Think,* 2nd ed. (Natick, MA: A.K. Peters, Ltd., 2004), ISBN 1-56881-205-1, Online Computer Library Center, Inc.

7. Navdeep Singh Gill, "Artificial Neural Networks, Neural Networks Applications and Algorithms," *Xenonstack,* July 21, 2017; Andrew L. Beam, "Deep Learning 101 - Part 1: History and Background" and "Deep Learning 101 - Part 2: Multilayer Perceptrons," *Machine Learning and Medicine,* February 23, 2017; and Andrej Karpathy, "CS231n: Convolutional Neural Networks for Visual Recognition," Stanford University Computer Science Class.

8. Beam, "Deep Learning 101 - Part 1" and "Deep Learning 101 - Part 2."

9. Karpathy, "CS231n."

10. Defense Advanced Research Projects Agency, "Toward Machines that Improve with Experience," March 16, 2017.

identify actions such as traffic accidents and violent crimes.

Another important aspect of AI is the ability to predict behavior. In contrast to the imaging and identification of criminal activity in progress, the University of Houston has used NIJ funding to develop algorithms that provide continuous monitoring to assess activity and predict emergent suspicious and criminal behavior across a network of cameras. This work also concentrates on using clothing, skeletal structure, movement, and direction prediction to identify and reacquire people of interest across multiple cameras and images.[15]

DNA analysis

AI can also benefit the law enforcement community from a scientific and evidence processing standpoint. This is particularly true in forensic DNA testing, which has had an unprecedented impact on the criminal justice system over the past several decades.

Biological material, such as blood, saliva, semen, and skin cells, can be transferred through contact with people and objects during the commission of a crime. As DNA technology has advanced, so has the sensitivity of DNA analysis, allowing forensic scientists to detect and process low-level, degraded, or otherwise unviable DNA evidence that could not have been used previously. For example, decades-old DNA evidence from violent crimes such as sexual assaults and homicide cold cases is now being submitted to laboratories for analysis. As a result of increased sensitivity, smaller amounts of DNA can be detected, which leads to the possibility of detecting DNA from multiple contributors, even at very low levels. These and other developments are presenting new challenges for crime laboratories. For instance, when using highly sensitive methods on items of evidence, it may be possible to detect DNA from multiple perpetrators or from someone not associated with the crime at all — thus creating the issue of DNA mixture interpretation and the need to separate and identify (or "deconvolute") individual profiles to generate critical investigative leads for law enforcement.

AI may have the potential to address this challenge. DNA analysis produces large amounts of complex data in electronic format; these data contain patterns, some of which may be beyond the range of human analysis but may prove useful as systems increase in sensitivity. To explore this area, researchers at Syracuse University partnered with the Onondaga County Center for Forensic Sciences and the New York City Office of Chief Medical Examiner's Department of Forensic Biology to investigate a novel machine learning-based method of mixture deconvolution. With an NIJ research award, the Syracuse University team worked to combine the strengths of approaches involving human analysts with data mining and AI algorithms. The team used this hybrid approach to separate and identify individual DNA profiles to minimize the potential weaknesses inherent in using one approach in isolation. Although ongoing evaluation of the use of AI techniques is needed and there are many factors that can influence the ability to parse out individual DNA donors, research shows that AI technology has the potential to assist in these complicated analyses.[16]

The National Artificial Intelligence Research and Development Strategic Plan

On May 3, 2016, the White House announced a series of actions to spur public dialogue on artificial intelligence (AI), identify challenges and opportunities related to this technology, aid in the use of AI for more effective government, and prepare for the potential benefits and risks of AI. As part of these actions, the White House directed the creation of a national strategy for AI research and development. Following is a summary of the plan's areas and intent.[1]

Manufacturing
- Increase U.S. manufacturing by using robotics
- Improve worker health and safety
- Improve product quality and reduce costs
- Accelerate production capabilities
- Improve demand forecasting
- Increase flexibility in operations and the supply chain
- Predict impacts to manufacturing operations
- Improve scheduling of processes and reduce inventory requirements

Logistics
- Improve supply chains with adaptive scheduling and routing
- Provide more robust supply chains

Finance
- Allow early detection of risk
- Reduce malicious behavior and fraud
- Increase efficiency and reduce volatility
- Prevent systemic failures

Transportation
- Improve structural health monitoring and infrastructure management
- Reduce the cost of repair and reconstruction
- Make vehicular travel safer
- Provide real-time route information
- Improve transportation networks and reduce emissions

Agriculture
- Improve production, processing, and storage
- Improve distribution and consumption of agricultural products
- Gather data about crops to remove weeds and pests more efficiently
- Apply treatments (water, fertilizer, etc.) strategically
- Fill labor gaps

Marketing
- Provide a better match of supply with demand
- Drive up revenue for private-sector development
- Anticipate consumer needs, and find products and services
- Reduce costs

Communications
- Maximize efficient bandwidth use
- Automate information storage and retrieval
- Improve filter, search, translation, and summarization functions

Science and Technology
- Assist in knowledge accumulation
- Refine theories
- Generate hypotheses and perform experiments using simulations

Education
- Provide automated tutoring and instruction
- Improve personalized programs and evaluation
- Provide life-long learning and new skills for the total population

Medicine
- Use bioinformatics to identify genetic risk from large-scale studies
- Predict safety and efficacy of pharmaceuticals
- Develop new pharmaceutical compounds
- Customize medicine
- Diagnose conditions and recommend treatment

Law
- Analyze case law history
- Assist with discovery process
- Summarize evidence

Personal Services
- Provide natural language systems for an easier interface and user experience
- Provide automated personal assistants
- Allow group scheduling

Security and Law Enforcement
- Detect patterns and anomalous behavior
- Predict crowd behavior and crime patterns
- Protect critical infrastructure
- Uncover criminal networks

Safety and Prediction
- Predict infrastructure disruptions with distributed sensor systems and pattern information
- Adapt operations for minimal impact

Note

1. Networking and Information Technology Research and Development Subcommittee of the National Science and Technology Council, *National Artificial Intelligence Research and Development Strategic Plan,* Office of Science and Technology Policy, October 2016, 8-11.

Gunshot detection

The discovery of pattern signatures in gunshot analysis offers another area in which to use AI algorithms. In one project, NIJ funded Cadre Research Labs, LLC, to analyze gunshot audio files from smartphones and smart devices "based on the observation that the content and quality of gunshot recordings are influenced by firearm and ammunition type, the scene geometry, and the recording device used."[17] Using a well-defined mathematical model, the Cadre scientists are working to develop algorithms to detect gunshots, differentiate muzzle blasts from shock waves, determine shot-to-shot timings, determine the number of firearms present, assign specific shots to firearms, and estimate probabilities of class and caliber — all of which could help law enforcement in investigations.[18]

Crime forecasting

Predictive analysis is a complex process that uses large volumes of data to forecast and formulate potential outcomes. In criminal justice, this job rests mainly with police, probation practitioners, and other professionals, who must gain expertise over many years. The work is time-consuming and subject to bias and error.[19]

With AI, volumes of information on law and legal precedence, social information, and media can be used to suggest rulings, identify criminal enterprises, and predict and reveal people at risk from criminal enterprises. NIJ-supported researchers at the University of Pittsburgh are investigating and designing computational approaches to statutory interpretation that could potentially increase the speed

and quality of statutory interpretation performed by judges, attorneys, prosecutors, administrative staff, and other professionals. The researchers hypothesize that a computer program can automatically recognize specific types of statements that play the most important roles in statutory interpretation. The goal is to develop a proof-of-concept expert system to support interpretation and perform it automatically for cybercrime.[20]

AI is also capable of analyzing large volumes of criminal justice-related records to predict potential criminal recidivism. Researchers at the Research Triangle Institute, in partnership with the Durham Police Department and the Anne Arundel County (Maryland) Sheriff's Office, are working to create an automated warrant service triage tool for the North Carolina Statewide Warrant Repository. The NIJ-supported team is using algorithms to analyze data sets with more than 340,000 warrant records. The algorithms form decision trees and perform survival analysis to determine the time span until the next occurrence of an event of interest and predict the risk of reoffending for absconding offenders (if a warrant goes unserved). This model will help practitioners triage warrant service when backlogs exist. The resulting tool will also be geographically referenced so that practitioners can pursue concentrations of high-risk absconders — along with others who have active warrants — to optimize resources.[21]

AI can also help determine potential elder victims of physical and financial abuse. NIJ-funded researchers at the University of Texas Health Science Center at Houston used AI algorithms to analyze elder victimization. The algorithms can determine the victim, perpetrator, and environmental factors that distinguish between financial exploitation and other forms of elder abuse. They can also differentiate "pure" financial exploitation (when the victim of financial exploitation experiences no other abuse) from "hybrid" financial exploitation (when physical abuse or neglect accompanies financial exploitation). The researchers hope that these data algorithms can be transformed into web-based applications so that practitioners can reliably determine the likelihood that financial exploitation is occurring and quickly intervene.[22]

Finally, AI is being used to predict potential victims of violent crime based on associations and behavior. The Chicago Police Department and the Illinois Institute of Technology used algorithms to collect information and form initial groupings that focus on constructing social networks and performing analysis to determine potential high-risk individuals. This NIJ-supported research has since become a part of the Chicago Police Department's Violence Reduction Strategy.[23]

The Future of AI in Criminal Justice

Every day holds the potential for new AI applications in criminal justice, paving the way for future possibilities to assist in the criminal justice system and ultimately improve public safety.

Video analytics for integrated facial recognition, the detection of individuals in multiple locations via closed-circuit television or across multiple cameras, and object and activity detection could prevent crimes through movement and pattern analysis, recognize crimes in progress, and help investigators identify suspects. With technology such as cameras, video, and social media generating massive volumes of data, AI could detect crimes that would otherwise go undetected and help ensure greater public safety by investigating potential criminal activity, thus increasing community confidence in law enforcement and the criminal justice system. AI also has the potential to assist the nation's crime laboratories in areas such as complex DNA mixture analysis.

Pattern analysis of data could be used to disrupt, degrade, and prosecute crimes and criminal enterprises. Algorithms could also help prevent victims and potential offenders from falling into criminal pursuits and assist criminal justice professionals in safeguarding the public in ways never before imagined.

AI technology also has the potential to provide law enforcement with situational awareness and context, thus aiding in police well-being due to better informed responses to possibly dangerous situations. Technology that includes robotics and drones could also perform public safety surveillance, be integrated

into overall public safety systems, and provide a safe alternative to putting police and the public in harm's way. Robotics and drones could also perform recovery, provide valuable intelligence, and augment criminal justice professionals in ways not yet contrived.

By using AI and predictive policing analytics integrated with computer-aided response and live public safety video enterprises, law enforcement will be better able to respond to incidents, prevent threats, stage interventions, divert resources, and investigate and analyze criminal activity. AI has the potential to be a permanent part of our criminal justice ecosystem, providing investigative assistance and allowing criminal justice professionals to better maintain public safety.

About the Author

Christopher Rigano is a senior computer scientist in NIJ's Office of Science and Technology.

This article discusses the following grants:

- "Design and Implementation of Forensic Facial Identification Experts Test," grant number 2015-IJ-CX-K014
- "A Simultaneous Low Resolution and Off-Pose Angle Face Matching Algorithm as an Investigative Lead Generative Tool for Law Enforcement," grant number 2013-IJ-CX-K005
- "Studying the Impact of Video Analytics for Pre, Live and Post Event Analysis on Outcomes of Criminal Justice," grant number 2015-R2-CX-K025
- "Learning Models for Predictive Behavioral Intent and Activity Analysis in Wide Area Video Surveillance," grant number 2009-MU-MU-K004
- "DeGrade It," grant number 2016-R2-CX-0012
- "A Hybrid Machine Learning Approach for DNA Mixture Interpretation," grant number 2014-DN-BX-K029
- "Development of Computational Methods for the Audio Analysis of Gunshots," grant number 2016-DN-BX-0183
- "A Recommendation System for Statutory Interpretation in Cybercrime," grant number 2016-R2-CX-0010
- "Applying Data Science To Justice Systems: The North Carolina Statewide Warrant Repository (NCAWARE)," grant number 2015-IJ-CX-K016
- "Elder Financial Exploitation Victimization," grant number 2013-IJ-CX-0050
- "Chicago Police Predictive Policing Demonstration and Evaluation Project," grant number 2011-IJ-CX-K014

Notes

1. Erik Brynjolfsson and Andrew McAfee, "The Business of Artificial Intelligence: What It Can — and Cannot — Do for Your Organization," *Harvard Business Review* (August 2017); and Giosué Lo Bosco and Mattia Antonino Di Gangi, "Deep Learning Architectures for DNA Sequence Classification," *Fuzzy Logic and Soft Computing Applications — 2017: Revised Selected Papers From the 11th International Workshop, WILF 2016, Naples, Italy, December 19-21, 2016,* eds. Alfredo Petrosino, Vincenzo Loia, and Witold Pedrycz (London: Springer Nature, 2018), 162-171, doi:10.1007/978-3-319-52962-2.
2. The Society for the Study of Artificial Intelligence and Simulation of Behaviour, "What is Artificial Intelligence."
3. Bernard Marr, "What Is the Difference Between Deep Learning, Machine Learning and AI?" *Forbes* (December 8, 2016).
4. National Science and Technology Council and the Networking and Information Technology Research and Development Subcommittee, *The National Artificial Intelligence Research and Development Strategic Plan,* Washington, DC: Office of Science and Technology Policy, October 2016, https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.
5. The Intelligence Advanced Research Projects Activity, "Janus," Washington, DC: Office of the Director of National Intelligence, https://www.iarpa.gov/index.php/research-programs/janus.
6. Yunlong Zhang and Lori M. Bruce, *Mississippi Transportation Research Center: Automated Accident Detection at Intersections* (Project Number: FHWA/MS-DOT-RD-04-150), Jackson, MS: Mississippi Department of Transportation and U.S. Department of Transportation Federal Highway Administration, March 2004.
7. Rachel Z. Arndt, "Artificial Intelligence Takes on Medical Imaging," *Transportation Hub* (July 8, 2017).
8. Brynjolfsson and McAfee, "The Business of Artificial Intelligence"; and Lo Bosco and Di Gangi, "Deep Learning Architecture for DNA Sequence Classification."
9. Ajit Jaokar, "Artificial Intelligence in Fraud Detection," *Envision Blog,* March 15, 2017.
10. Eric Knorr, "How PayPal Beats the Bad Guys With Machine Learning," Ahead of the Curve, *InfoWorld* (April 13, 2015).

11. "Design and Implementation of Forensic Facial Identification Experts Test" at the University of Texas at Dallas, NIJ award number 2015-IJ-CX-K014; and P. Jonathon Phillips, "A Cross Benchmark Assessment of a Deep Convolutional Neural Network for Face Recognition," paper presented at the 12th IEEE International Conference on Automatic Face & Gesture Recognition, 2017, 705-710.
12. "A Simultaneous Low Resolution and Off-Pose Angle Face Matching Algorithm as an Investigative Lead Generative Tool for Law Enforcement" at Carnegie Mellon University, NIJ award number 2013-IJ-CX-K005.
13. "DeGrade It" at Dartmouth College, NIJ award number 2016-R2-CX-0012.
14. "Studying the Impact of Video Analytics for Pre, Live and Post Event Analysis on Outcomes of Criminal Justice" at the University of Central Florida, NIJ award number 2015-R2-CX-K025.
15. "Learning Models for Predictive Behavioral Intent and Activity Analysis in Wide Area Video Surveillance" at the University of Houston, NIJ award number 2009-MU-MU-K004.
16. "A Hybrid Machine Learning Approach for DNA Mixture Interpretation" at Syracuse University, NIJ award number 2014-DN-BX-K029.
17. "Detailed Information for Award 2016-DN-BX-0183," National Institute of Justice, https://external.ojp.usdoj.gov/selector/awardDetail?awardNumber=2016-DN-BX-0183&fiscalYear=2016&applicationNumber=2016-90227-IL-IJ&programOffice=NIJ&po=NIJ.
18. "Development of Computational Methods for the Audio Analysis of Gunshots" at Cadre Research Labs, LLC, NIJ award number 2016-DN-BX-0183.
19. See, for example, "Effects of Human Factors on the Accuracy of Fingerprint Analysis," National Institute of Justice, https://nij.gov/topics/forensics/evidence/impression/Pages/human-factors.aspx.
20. "A Recommendation System for Statutory Interpretation in Cybercrime" at the University of Pittsburgh, NIJ award number 2016-R2-CX-0010.
21. "Applying Data Science to Justice Systems: The North Carolina Statewide Warrant Repository (NCAWARE)" at RTI International, NIJ award number 2015-IJ-CX-K016.
22. "Exploring Elder Financial Exploitation Victimization" at the University of Texas Health Science Center at Houston, NIJ award number 2013-IJ-CX-0050.
23. "Chicago Police Predictive Policing Demonstration and Evaluation Project" at the Chicago Police Department and Illinois Institute of Technology, NIJ award number 2011-IJ-CX-K014.

Image source: Erika Cross, Frenzel, GaudiLab, ESB Professional, and Jerome Scholler/Shutterstock; Maxiphoto/iStock

---

NCJ 252038

Cite this article as: Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs," *NIJ Journal* 280, January 2019, https://www.nij.gov/journals/280/Pages/using-artificial-intelligence-to-address-criminal-justice-needs.aspx.

Accessibility Report

Filename:
05-280_indiv_AI_for web.pdf

Report created by:

Organization:

[Enter personal and organization information through the Preferences > Identity dialog.]

Summary

The checker found no problems in this document.

- Needs manual check: 0
- Passed manually: 2
- Failed manually: 0
- Skipped: 0
- Passed: 30
- Failed: 0

Detailed Report

Document

Rule Name	Status	Description
Accessibility permission flag	Passed	Accessibility permission flag must be set
Image-only PDF	Passed	Document is not image-only PDF
Tagged PDF	Passed	Document is tagged PDF
Logical Reading Order	Passed manually	Document structure provides a logical reading order
Primary language	Passed	Text language is specified
Title	Passed	Document title is showing in title bar
Bookmarks	Passed	Bookmarks are present in large documents
Color contrast	Passed manually	Document has appropriate color contrast

Page Content

Rule Name	Status	Description
Tagged content	Passed	All page content is tagged
Tagged annotations	Passed	All annotations are tagged
Tab order	Passed	Tab order is consistent with structure order
Character encoding	Passed	Reliable character encoding is provided
Tagged multimedia	Passed	All multimedia objects are tagged
Screen flicker	Passed	Page will not cause screen flicker
Scripts	Passed	No inaccessible scripts
Timed responses	Passed	Page does not require timed responses
Navigation links	Passed	Navigation links are not repetitive

Forms

Rule Name	Status	Description
Tagged form fields	Passed	All form fields are tagged
Field descriptions	Passed	All form fields have description

Alternate Text

Rule Name	Status	Description
Figures alternate text	Passed	Figures require alternate text

Nested alternate text	Passed	Alternate text that will never be read
Associated with content	Passed	Alternate text must be associated with some content
Hides annotation	Passed	Alternate text should not hide annotation
Other elements alternate text	Passed	Other elements that require alternate text

Tables

Rule Name	Status	Description
Rows	Passed	TR must be a child of Table, THead, TBody, or TFoot
TH and TD	Passed	TH and TD must be children of TR
Headers	Passed	Tables should have headers
Regularity	Passed	Tables must contain the same number of columns in each row and rows in each column
Summary	Passed	Tables must have a summary

Lists

Rule Name	Status	Description
List items	Passed	LI must be a child of L
Lbl and LBody	Passed	Lbl and LBody must be children of LI

Headings

Rule Name	Status	Description
Appropriate nesting	Passed	Appropriate nesting

Back to Top

From: Holz, Jordan
Sent: Tue, 12 May 2020 20:13:25 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: ICE Monthly Report
Attachments: ICE Privacy Report, Operational Only, 20200501.pdf, ICE Monthly Status Report, April 2020.pdf

Hi (b)(6); (b)(7)(C)

Can you save these to the shared drive?

Copying Jen to compare the monthly report against our PTA tracker, which I'm hoping to eventually put onto our new SharePoint page.

Jordan Holz
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-(b)(6);
Mobile: 202-701(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) @hq.dhs.gov>
Sent: Tuesday, May 12, 2020 4:04 PM
To: Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov>
Cc: PIA <PIA@HQ.DHS.GOV>
Subject: ICE Monthly Report

Good afternoon,

Please find attached the latest ICE Monthly Report and Crystal Report. Please let me know of any inaccuracies you may find in the reports.

Respectfully,

(b)(6); (b)(7)(C)
Privacy Analyst
Contractor supporting the DHS Privacy Office
Phone: (202) 343-(b)(6);
Email: (b)(6); (b)(7)(C) @associates.hq.dhs.gov

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

ICE Monthly Privacy Status Report

The following information is a comprehensive list of Privacy documentation with the DHS Privacy Office as of **05/11/20**.

Any correspondence received after **05/11/20** may not be captured on this report.

I. Federal Information Security Management Act (FISMA) Reporting:

a. PIAs: 100%

b. SORNs: 100%

II. Privacy Threshold Analysis (PTA):

PTAs Approved by PRIV Last Month **14**

Name	Acronym	Received	Approved	PIA/SORN Required	Expiration
IT Service Management Transition Project	ISTP	6/21/2017	4/1/2020	A PIA is required: A new PIA is required SORN Coverage to be determined	4/1/2021
Enterprise Operations Center (EOC)	EOC	3/25/2020	4/2/2020		4/2/2023
I-901 Fee Collection Services System	I-901	3/30/2020	4/2/2020		4/2/2023
Collabware – Collabspace Pilot	SEVPAMS	4/1/2020	4/2/2020		4/2/2023
ICE Cloud General Support System (GSS)	ICE Cloud GSS	4/1/2020	4/2/2020		4/2/2023
HSI Use of DHS OBIM's IDENT Facial Recognition Systems		3/24/2020	4/2/2020	A PIA is required: A new PIA is required A SORN is required: SORN update is required	4/2/2021
ICE Financial Analytics System	IFAS	3/16/2020	4/6/2020		4/6/2023
HSI Analytical Applications		4/8/2020	4/8/2020		
Team Awareness Kit (TAK)	TAK	3/17/2020	4/20/2020	A PIA is required: A new PIA is required	4/20/2021
Department of Homeland Security (DHS) Analysis		4/21/2020	4/21/2020		4/21/2023
Removal Management Division Deferred Action Program	ICECT	4/8/2020	4/24/2020		4/24/2023
287(g) Program Needs Assessment	287(g) PNA	4/24/2020	4/27/2020		4/27/2023
Alien Criminal Response Information Management System (ACRIMe) v. 5.4	ACRIMe	4/29/2020	4/30/2020		4/30/2023
Forensic Interview Program Database	HSI	4/21/2020	4/30/2020		4/30/2023

PTAs Currently in Review **9**

Name	Acronym	Received	Location
Child Exploitation Mobile Application		8/25/2017	Complete
ClearView AI		2/27/2020	With Analyst
Fugitive Tracking System	HSI	12/17/2018	With Component
HSI International Visitors Program SharePoint Application	HSI	3/11/2019	With Component
HSI Use of State Facial Recognition Systems	HSI FRS	12/27/2019	With Analyst
National Capitol Region Gang Intelligence System	NCR GIS	10/29/2019	With Analyst
Newman Analytical Tool	Newman	4/2/2019	With Component

Non-Telephonic Inquiries Tracking System (NTIS)	NTIS	4/7/2020	With Component
Venntel Geolocation Data Subscriptions	Venntel	9/18/2019	With Analyst

III. Privacy Impact Assessment (PIA):

PIAs Approved Last Month **1**

Name	Acronym	Approved	Published
DHS/ICE/PIA-043 SharePoint Matter Tracking Systems		4/13/2020	4/13/2020

PIAs in Review with DHS Privacy **7**

Name	Acronym	Received	Location
DHS/ICE/PIA-044 LeadTrac	LeadTrac	3/8/2020	With Director
DHS/ICE/PIA-XXX Angel Watch Program		4/28/2020	With Component
DHS/ICE/PIA-XXX Biometric Identification Transnational Migration Alert Program	BITMAP	10/28/2019	With Analyst
DHS/ICE/PIA-XXX ICE Use of Facial Recognition Services		3/27/2020	With DCPO
DHS/ICE/PIA-XXX Repository for Analytics in a Virtualized Environment	RAVEN	1/23/2020	With DCPO
DHS/ICE/PIA-XXX Undercover Operations Unit Modernization	UOU	5/7/2020	With Analyst
DHS/ICE/PIA-XXX War Crime Hunter		1/30/2020	With Director

PIAs Required by PTAs **20**

Name	Acronym	New/Update	PTA Name	PTA Approved
DHS/ICE/PIA-XXX ICE Use of Facial Recognition Services		A PIA is required: A new PIA is required	HSI Use of DHS OBIM's IDENT Facial Recognition Systems	4/2/2020
DHS/ALL/PIA-020 Financial Disclosure Management	FDM	A PIA is required: A new PIA is required	Financial Disclosure OnLine	7/22/2019
DHS/ICE/PIA-051 Law Enforcement Information Sharing Service	LEIS Service	A PIA is required: A new PIA is required	Biometric International Query Service Phase I	3/15/2019
DHS/ICE/PIA-XXX ERO Custody Programs		A PIA is required: A new PIA is required	LGBTI ECCO/JIC Status Tracker	12/6/2019
DHS/ICE/PIA-044 LeadTrac System	LeadTrac System	PIA Appendix Required	LeadTrac Modernization	11/24/2019
DHS/ICE/PIA-XXX ERO Custody Programs		A PIA is required: A new PIA is required	Disabilities Case Tracker	12/6/2019
DHS/ALL/PIA-080 DNA Collection		A PIA is required: A new PIA is required	ICE NDIS/CODIS DNA Collection	12/4/2019
DHS/ICE/PIA-XXX IT Service Management Transition Project		A PIA is required: A new PIA is required	IT Service Management Transition Project	4/1/2020
DHS/ICE/PIA-XXX Repository for Analytics in a Virtualized Environment		PIA Appendix Required	Criminal Research Analytic Networked Environment I-GROOT	5/11/2020
DHS/ICE/PIA-037 Electronic Health Records System	eHR	A PIA is required: A new PIA is required	Electronic Health Records	6/26/2019
DHS/ICE/PIA-XXX Repository for Analytics in a Virtualized Environment		A PIA is required: A new PIA is required	Vulture	11/17/2019
DHS/ICE/PIA-XXX ERO Custody Programs		A PIA is required: A new PIA is required	Parental Interests Portfolio Data Tracker	12/6/2019
DHS/ALL/PIA-XXX Team Awareness Kit		A PIA is required: A new PIA is required	Team Awareness Kit (TAK)	4/20/2020
DHS/ICE/PIA-044 LeadTrac System	LeadTrac System	A PIA is required: A PIA update is required	LeadTrac Modernization	11/24/2019
DHS/ALL/PIA-072 National Vetting Center	NVC	PIA Appendix Required	ICE Support of Non-Immigrant Visa Vetting at the NVC using CBP's ATS/UPAX	3/1/2020
DHS/ICE/PIA-XXX DICE		A PIA is required: A new PIA is required	Criminal Research Analytic Networked Environment I-GROOT	5/11/2020
DHS/ICE/PIA-XXX Homeland Security Investigations Citizens Academy		A PIA is required: A new PIA is required	Citizens Academy Application and Nomination Forms	12/3/2019
DHS/ICE/PIA-XXX Repository for Analytics in a Virtualized Environment		A PIA is required: A new PIA is required	Criminal Research Analytic Networked Environment I-GROOT	5/11/2020

DHS/ALL/PIA-043 DHS Hiring and On-Boarding Process	H&O	PIA Appendix Required	Medical Examination and History Report	1/13/2020
DHS/ICE/PIA-XXX Undercover Operations Unit Modernization		A PIA is required: A new PIA is required	Undercover Operations Unit Modernization	10/7/2019

IV. System of Records Notice (SORN):

SORNs Approved Last Month **0**

Name	Approved	Published

SORNs in Review **3**

Name	Received	Location
DHS/ICE-012 Visa Security Program Tracking System-Network	7/26/2009	Complete
DHS/ICE-005 Trade Transparency Analysis and Research	10/12/2018	With Component
DHS/ICE-001 Student and Exchange Visitor Program	9/21/2018	With Analyst

SORNs Identified by PTA **10**

Name	New/Update	PTA Name	PTA Approved
DHS/ICE-013 Alien Health Records	A SORN is required: A new SORN is required	Medical Related Incident Reporting Tool	1/8/2019
DHS/ICE-009 External Investigations	A SORN is required: SORN update is required	HSI Use of DHS OBIM's IDENT Facial Recognition Systems	4/2/2020
DHS/ICE-004 Bond Management Information System	A SORN is required: A new SORN is required	Bond Management Information System Web	8/24/2018
DHS/ICE-XXX Custody Programs and Community Outreach	A SORN is required: A new SORN is required	LGBTI ECCO/JIC Status Tracker	12/6/2019
DHS/ICE-XXX Custody Programs and Community Outreach	A SORN is required: A new SORN is required	Disabilities Case Tracker	12/6/2019
DHS/ICE-XXX Custody Programs and Community Outreach	A SORN is required: A new SORN is required	Parental Interests Portfolio Data Tracker	12/6/2019
DHS/ALL-004 General Information Technology Access Account	A SORN is required: A new SORN is required	Cloud Collaboration and Software Suite	3/5/2018
DHS/ICE-XXX Homeland Security Investigations Citizens Academy	A SORN is required: A new SORN is required	Citizens Academy Application and Nomination Forms	12/3/2019
DHS/ALL-004 General Information Technology Access Account	A SORN is required: A new SORN is required	Cloud Collaboration and Software Suite	7/7/2017
DHS/ICE-009 External Investigations	A SORN is required: A new SORN is required	CrossTalk Chrome Extension	3/19/2018

From: (b)(6); (b)(7)(C)
Sent: Mon, 24 Feb 2020 21:50:19 +0000
To: (b)(6); (b)(7)(C)
Subject: FW: Privacy Weekly Newsletter

I was thinking of SEN use (e.g. Clearview facial recognition technology) with C3/CEIU in the following context spelled out in the SEN PIA:

"OPPRED: The Operation PREDATOR (OPPRED) Significant Incident Arrest Report is essentially the same as the SIR but is used only when the incident involves a subject who committed a sexually-based crime against a victim under the age of 18. OPPREDs capture some additional information pertaining to the victim and the suspect to capture more specific information in crimes against children (p. 3)."
(b)(7)(E)

"OPPRED: OPPREDs include the same information as the SIR. Additionally, they include criminal history information (such as city and state of arrest, registered sex offender status, Amber Alert association status, PROTECT Act case relevance status, aggravated felon status, fugitive status, prior arrest and conviction information), limited victim information (such as age group, sex, whether the individual was the victim of smuggling or trafficking, offender relationship to victim, country of birth, and country of citizenship), and contact information for the reporting ICE personnel, their supervisor, and the action officer and other law enforcement personnel who were notified. (p. 5)"
(b)(7)(E)

(b)(6); (b)(7)(C)
Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 732 (b)(6); (b)(7)(C)
Main: (202) 732

From: (b)(6); (b)(7)(C)
Sent: Monday, February 24, 2020 3:23 PM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>
Subject: FW: Privacy Weekly Newsletter

I asked (b)(6); (b)(7)(C) if he knew any connection between SEN use, facial recognition, CEIU, and child exploitation. (b)(6); (b)(7)(C) said he didn't know of any.

(b)(6); (b)(7)(C)
Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 732 (b)(6); (b)(7)(C)

Main: (202) 732(b)(6);

From: Holz, Jordan (b)(6); (b)(7)(C) ice.dhs.gov>
Sent: Monday, February 24, 2020 10:32 AM
To: (b)(6); (b)(7)(C) ice.dhs.gov>; (b)(6); (b)(7)(C) e.dhs.gov>;
(b)(6); (b)(7)(C) e.dhs.gov>; (b)(6); (b)(7)(C) e.dhs.gov>;
(b)(6); (b)(7)(C) ce.dhs.gov>; [redacted] ice.dhs.gov>;
(b)(6); (b)(7)(C) associates.ice.dhs.gov>; (b)(6); (b)(7)(C) (CTR)
(b)(6); (b)(7)(C) @associates.ice.dhs.gov>; (b)(6); (b)(7)(C) ociates.ice.dhs.gov>;
(b)(6); (b)(7)(C) ice.dhs.gov>
Subject: Privacy Weekly Newsletter

Good morning,

I hope everyone had a nice weekend. I wanted to give you all a quick update on some recent Privacy Division/IGP news since the last time we all met:

1. **License Plate Reader Enhancements**: Last week, the vendor who provides ICE with access to its license plate reader query database came to PCN to demo its "geographic search" function. (b)(5)

2. **Published PIA**: Congratulations to (b)(6); r getting a PIA published!!! Completing the update to our Student Exchange and Visitor Program (SEVP) PIA was a time-consuming endeavor, and Nicole did a great job coordinating everything between the program, OPLA, and DHS Privacy. The PIA can be found her (b)(7)(E) (b)(7)(E)

3. **Declined Detainer Reports**: Privacy continues to receive declined detainer reports from the Director's Office and ERO leadership to highlight cases where local jurisdictions would not cooperate with ICE. Generally, these cases highlight individuals who have been charged with (or convicted of) serious/violent offenses. One such individual went on to murder a 92-year-old in New York: https://www.nytimes.com/2020/01/14/nyregion/92-year-old-woman-queens-murder.html. Thanks to (b)(6); (b)(7)(C) or conducting initial reviews of these cases.

4. **Clearview Facial Recognition Technology**: The HSI Child Exploitation Investigations Unit (CEIU) has purchased facial recognition software from a company called Clearview to try and identify child predators. (b)(5) (b)(5) (b)(6); has drafted a PTA to document ICE's use of Clearview, and we will submit this to DHS if/when we receive guidance.

5. **IGP Town Hall**: As a reminder, IGP will have its quarterly town hall on **Wednesday February 26 at 2:00 PM** downstairs in the Julie Myers Conference Center (and via VTC). Please plan to attend.

Please let me know if you have any questions on the above items, or if you'd like me to add anything to next week's email.

Jordan Holz
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-(b)(6); (b)(7)(C)
Mobile: 202-70
Main: 202-732(b)(6);

From: (b)(6); (b)(7)(C)
Sent: Tue, 10 Jul 2018 15:13:12 +0000
To: (b)(6); (b)(7)(C)
Subject: Artificial Intelligence & Machine Learning Community of Interest Kick-Off Meeting

Artificial Intelligence & Machine Learning Community of Interest Kick-Off Meeting
What role can the Department play in the world of artificial intelligence (AI) and machine learning (ML)? Are you interested in exploring the possibilities and opportunities that this burgeoning field may hold for DHS?

S&T recently launched a DHS-wide Artificial Intelligence/Machine Learning Community of Interest (COI) SharePoint site to exchange information and encourage collaboration within DHS about this exciting, growing field. Join S&T Chief Scientis(b)(6); (b)(7)(C) or an informative session about this AI/ML Community of Interest:

Date: July 11, 2018
Time: 9 a.m. - 11a.m.
Location: VTA, 8- ABC

Via Webinar:

Meeting Link: https://share.dhs.gov/aimlcoi/

Conference Number: 877-686-1425

Participant Code: 8376138
Test your connection: https://share.dhs.gov/common/help/en/support/meeting_test.htm
Need a brief overview? http://www.adobe.com/products/adobeconnect.html

The COI is striving to:

- increase knowledge and understanding of AI/ML across the Department
- compare component needs and requirements in gathering, managing and analyzing large amounts of data, and
- facilitate collaborative R&D initiatives within the Department

(b)(6); (b)(7)(C) confident that the evolving and innovative field of AI/ML holds significant potential for DHS, for example, in areas related to efficiencies in collecting and interpreting massive amounts of data generated by interconnected systems. Also worthy of study is the topic of how advances in AI/ML can open the door to risks and challenges from hostile systems designed to attack our systems. Privacy issues related to gathering personal information are also on the front burner.
DHS personnel from all components are encouraged to join the AI/ML COI community or to attend the first kick-off meeting in-person or via webinar. This is a chance for the COI members to connect in-person and collaborate. **If you plan to attend in-person, please contact the Office of the Chief Scientist at OCS@hq.dhs.gov.**

The OCS team is working to create a more robust site in the future, which will include

From: (b)(6); (b)(7)(C)
Sent: Fri, 7 Feb 2020 20:37:35 +0000
To: (b)(6); (b)(7)(C)
Subject: Davey Alba, New York Times, "NY school district adopts facial-recognition tech"

This article does not necessarily represent my views, but it would be interesting if this could ever come up in the Significant Event Notification (SEN) System context.

(b)(5)

(b)(6); (b)(7)(C)
Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 73 (b)(6); (b)(7)(C)
Main: (202) 73

From: (b)(6); (b)(7)(C)
Sent: Tue, 11 Feb 2020 21:45:41 +0000
To: (b)(6); (b)(7)(C)
Subject: FW: Article on state drivers license photos and facial recognition

"The FBI and Immigration and Customs Enforcement (ICE) have reportedly been using driver's license photos for facial recognition searches without license holders' knowledge or consent. The Washington Post reports the two agencies have used millions of Americans' photos, largely from driver's licenses, for the purpose of facial recognition searches, citing internal documents and emails from the two agencies that were obtained by Georgetown Law researchers over the past five years and shared with the news outlet." https://thehill.com/policy/technology/451913-fbi-ice-using-state-drivers-license-photos-without-consent-to-create-facial

(b)(6); (b)(7)(C)
Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 732-(b)(6); (b)(7)(C)
Main: (202) 732-

From: Holz, Jordan <(b)(6); (b)(7)(C)@ice.dhs.gov>
Sent: Monday, July 8, 2019 8:59 AM
T(b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>;
(b)(6); (b)(7)(C)ce.dhs.gov>; (b)(6); (b)(7)(C)ice.dhs.gov>;
(b)(6); (b)(7)(C)ice.dhs.gov>; (b)(6); (b)(7)(C)CTR)
(b)(6); (b)(7)(C)associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>
Subject: RE: Article on state drivers license photos and facial recognition

Thanks (b)(6); (b)(7)(C)'ll probably be discussing this issue with OPLA later this afternoon.

Jordan Holz, J.D., CIPP/US/G
Acting Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-(b)(6); (b)(7)(C)
Mobile: 202-70
Main: 202-732-(b)(6);

Questions? Please visit our website at https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx

From: (b)(6); (b)(7)(C)
Sent: Monday, July 8, 2019 8:48 AM
To: Holz, Jordan (b)(6); (b)(7)(C) ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @associates.ice.dhs.gov>;
(b)(6); (b)(7)(C) associates.ice.dhs.gov>
Subject: Article on state drivers license photos and facial recognition

https://thehill.com/policy/technology/451913-fbi-ice-using-state-drivers-license-photos-without-consent-to-create-facial

From (b)(6); (b)(7)(C)
Sent: Wednesday, May 22, 2019 5:19 PM
To: Holz, Jordan (b)(6); (b)(7)(C) ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) e@ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) ice.dhs.gov (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6);
(b)(6); (b)(7)(C) @associates.ice.dhs.gov>; (b)(6); (b)(7)(C) (CTR)
(b)(6); (b)(7)(C) associates.ice.dhs.gov>; (b)(6); (b)(7)(C) associates.ice.dhs.gov>
Subject: RE: Article on Facial Recognition Technology

https://thehill.com/policy/technology/445095-lawmakers-call-for-time-out-on-facial-recognition-tech

From: (b)(6); (b)(7)(C)
Sent: Wednesday, May 22, 2019 10:28 AM
To: Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) @ice.dhs.gov> (b)(6); (b)(7)(C) ice.dhs.gov>;
(b)(6); (b)(7)(C) ce.dhs.gov>; (b)(6); (b)(7)(C) .dhs.gov> (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) associates.ice.dhs.gov (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) sociates.ice.dhs.gov>; (b)(6); (b)(7)(C) associates.ice.dhs.gov>
Subject: RE: Article on Facial Recognition Technology

It just started https://www.youtube.com/watch?v=jLmzEFkbNsg

From: (b)(6); (b)(7)(C)
Sent: Wednesday, May 22, 2019 10:19 AM
To: Holz, Jordan (b)(6); (b)(7)(C) ce.dhs.gov (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) ice.dhs.gov> (b)(6); (b)(7)(C) ice.dhs.gov> (b)(6);
(b)(6); (b)(7)(C) associates.ice.dhs.gov> (b)(6); (b)(7)(C) TR)
(b)(6); (b)(7)(C) associates.ice.dhs.gov> (b)(6); (b)(7)(C) sociates.ice.dhs.gov>
Subject: RE: Article on Facial Recognition Technology

https://www.youtube.com/watch?v=Ep5jalDX-oo This works

From: (b)(6); (b)(7)(C)
Sent: Wednesday, May 22, 2019 10:03 AM
To: Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) e@ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) @ice.dhs.gov> (b)(6); (b)(7)(C) ice.dhs.gov> (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) ssociates.ice.dhs.gov> (b)(6); (b)(7)(C) TR)
(b)(6); (b)(7)(C) @associates.ice.dhs.gov> (b)(6); (b)(7)(C) ociates.ice.dhs.gov>
Subject: RE: Article on Facial Recognition Technology

This is the link https://www.youtube.com/watch?v=jLmzEFkbNsg. It starts in a few minutes.

From: (b)(6); (b)(7)(C)
Sent: Wednesday, May 22, 2019 9:48 AM
To: Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>;
(b)(6); (b)(7)(C) e@ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>;
ice.dhs.gov> (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C) ssociates.ice.dhs.gov> (b)(6); (b)(7)(C) (CTR)
(b)(6); (b)(7)(C) @associates.ice.dhs.gov> (b)(6); (b)(7)(C) ociates.ice.dhs.gov>
Subject: RE: Article on Facial Recognition Technology

Washington, D.C. (May 21, 2019)—On Wednesday, May 22, 2019, the Committee will hold a hearing on "Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties."

WHERE: 2154 Rayburn House Office Building

WHEN: Wednesday, May 22, 2019

TIME: 10:00 a.m.

A livestream will be broadcast here.

https://oversight.house.gov/news/press-releases/committee-to-examine-the-impact-of-facial-recognition-technology-on-civil-rights

From: (b)(6); (b)(7)(C)
Sent: Tuesday, May 21, 2019 4:35 PM

To: Holz, Jordan <(b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>
Subject: RE: Article on Facial Recognition Technology

"There are currently no federal regulations regarding the use of facial recognition technology for commercial or government use." https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-20190522-SD002.pdf

---

From: (b)(6); (b)(7)(C)
Sent: Thursday, May 16, 2019 9:20 AM
To: Holz, Jorda(b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; P(b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; S(b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>
Subject: RE: Article on Facial Recognition Technology

https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html

---

From: Holz, Jordan
Sent: Wednesday, May 15, 2019 8:18 AM
To: (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>; (b)(6); (b)(7)(C)@associates.ice.dhs.gov>
Subject: Article on Facial Recognition Technology

FYI

https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html

Jordan Holz, J.D., CIPP/US/G
Deputy Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732(b)(6); (b)(7)(C)
Mobile: 202-7
Main: 202-732(b)(6);

Questions? Please visit our website at https://insight.ice.dhs.gov/mgt/igp/privacy/Pages/index.aspx

From: (b)(6); (b)(7)(C)
Sent: Thu, 5 Mar 2020 15:12:16 +0000
To: Holz, Jordan
Cc: PIA (b)(6); (b)(7)(C)
Subject: ICE Monthly Component Status Report & Crystal Privacy Report
Attachments: ICE - Monthly Status Report - February 2020.pdf, ICE Crystal Privacy Report, 20200304.pdf

Good afternoon,

I have attached the PRIV Monthly Component Status Report, which is current as of COB March 4, 2020. The attached Crystal Report is current as of March 4. If you have any questions or see anything that is inaccurate, please let me know—I used our new tracking system to produce this report, so things might look a little different.

Respectfully,

(b)(6); (b)(7)(C)
Privacy Analyst
DHS Privacy Office
Phone: (202) 343 (b)(6); (b)(7)(C)
Email: (b)(6); (b)(7)(C) @hq.dhs.gov