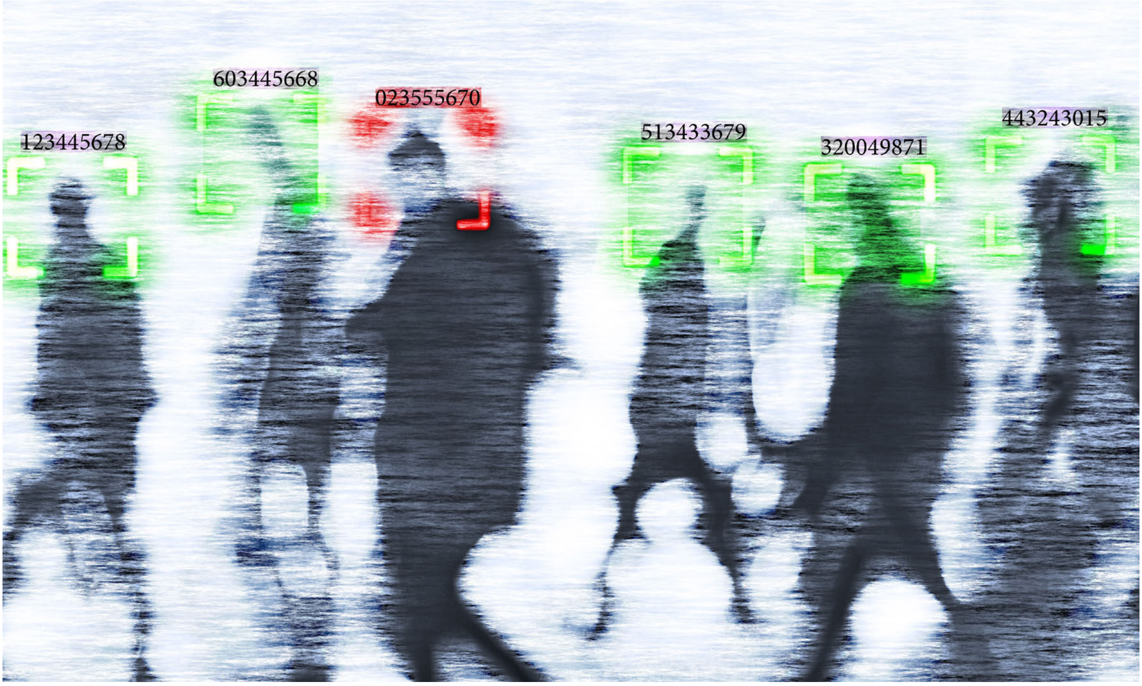


Public Perceptions of Artificial Intelligence for Homeland Security

BENJAMIN BOUDREAUX, DOUGLAS YEUNG, RACHEL STERATORE, THOMAS EDWARD GOODE, NIDHI KALRA, SYDNE J. NEWBERRY, MICHAEL W. ROBBINS, NATALIA HENRIQUEZ SANCHEZ, KELLER SCHOLL, VICTORIA M. SMITH, KRISTIN WARREN

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

An FFRDC operated by the RAND Corporation under contract with DHS

This research was published in 2024.

About This Report

To ensure that the U.S. Department of Homeland Security (DHS) can effectively integrate artificial intelligence (AI) into its missions, the department must evaluate the public's perceptions of DHS use of AI. In this study, researchers used a nationally representative survey to evaluate the American public's views of DHS use of AI. The insights and recommendations from this study will help DHS officials and other key stakeholders understand and integrate public perception into technology deployments.

This research was sponsored by the Science and Technology Directorate under contract HSHQDC-16-D-00007 and conducted in the Management, Technology, and Capabilities Program of the RAND Homeland Security Research Division, which operates the Homeland Security Operational Analysis Center (HSOAC). The research reported here was completed in March 2023 and underwent sensitive information review with the sponsor and the DHS Science and Technology Directorate (S&T) before public release.

About the Homeland Security Operational Analysis Center

The Homeland Security Act of 2002 (Public Law 107-296, § 305, as codified at 6 U.S.C. § 185), authorizes the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. The RAND Corporation operates HSOAC as an FFRDC for DHS under contract HSHQDC-16-D-00007.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. The HSOAC FFRDC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. The HSOAC FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under task order 70RSAT20FR0000089, Public Perception of Emerging Technology.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information on the RAND Homeland Security Research Division, see www.rand.org/hsrd.

For more information on this publication, see www.rand.org/t/RRA691-1.

Acknowledgments

We would like to thank Kathleen Deloughery, Ross Owens, and Sarah Perlstein from the Science and Technology Directorate. We also thank the DHS personnel who graciously shared their insights that informed the development of the survey. David Grant, Karen Edwards, and Lisa Wagner of the RAND American Life Panel provided invaluable assistance in fielding the survey and analyzing the data. We also thank our reviewers, Michael S. Pollard and Andrew J. Lohn, for excellent feedback that improved this report. In addition, we greatly appreciate the editing by Lisa Bernard. Lastly, this report would not have been possible without the guidance and support of Emma Westerman, Kelly Klima, and many others at the Homeland Security Operational Analysis Center.

Summary

Artificial intelligence (AI) systems, such as those that can recognize human faces or assess the likelihood that an event might occur, could be crucial in supporting the U.S. Department of Homeland Security's (DHS's) core missions.[1] DHS already uses AI in homeland security missions, such as in border and airport security and with criminal investigations, and it is actively seeking to further integrate emerging AI capabilities in other applications across DHS components.

However, the full potential of DHS use of emerging AI technologies is subject to several constraints, one of which is how key stakeholders (such as members of Congress, technology companies, and advocacy groups) and the public at large view government use of those technologies. Public perception of government use of technology is important for several reasons, such as to establish trust in and legitimacy of the government, to facilitate necessary funding and legislative support from Congress, and to foster collaboration with technology companies and operational partners.

Some of these key stakeholders have raised concerns about DHS use of AI technologies, including risks that DHS applications violate privacy and civil liberties, exacerbate inequity, and lack appropriate oversight and other safeguards. These concerns could shape or restrict DHS use of technology, so it is important that DHS understand the extent to which the public agrees with the department's approach to addressing these concerns.

In this research, we sought to evaluate public perception of the benefits and risks of DHS use of AI technologies.

Approach

Our approach to evaluating public perception of DHS use of AI involved a literature scan, interviews with DHS officials, and the development and deployment of a nationally representative survey of the American public. The survey was developed in 2020 and contained questions about current and planned DHS use of AI technologies, with a focus on four types of technologies: face recognition technology (FRT), license plate–reader technology, risk-assessment technology (e.g., algorithms that predict whether an event, such as an attack, will occur), and mobile phone location data. The survey was fielded using the RAND American Life Panel, a nationally representative panel of the American public, after we completed the procedural requirements of the Paperwork Reduction Act in October and November 2022.

[1] According to the DHS AI strategy, *AI* refers to "automated, machine-based technologies with at least some capacity for self-governance that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments" (DHS, 2020). *AI* is also often defined as a computer's ability to do things that are normally associated with human intelligence.

Key Findings

Key findings from the nationally representative survey include the following:

- Significant numbers of respondents might not have formed opinions about government use of FRT.
- Respondents said that security, accuracy, and privacy were more important than speed or convenience for government use of FRT.
- Respondents reported agreement that the government's use of FRT had both benefits and risks, but they were likelier to acknowledge risks than benefits.
- Respondents reported agreement that the government's use of FRT raised multiple types of risk, including misuse, inaccuracy, and bias.
- Less than one-quarter of the panel reported trusting the government's use of FRT.
- Safeguards could improve the public's comfort with government use of FRT, but these safeguards' overall effect on comfort levels might be limited.
- Respondents reported agreement that government must meet certain requirements for using FRT.
- Public support depends more on the application than on the technology.
- Respondents reported supporting some government applications of FRT (such as criminal investigations) but not others (such as identifying people at protests or public spaces).
- Respondents' reported support for risk technologies varied by application and data source.
- Respondents' reported support for license plate readers and mobile phone location data varied by government application.

Recommendations

Our findings underpin several specific recommendations. We recommend that DHS do the following:

- Proactively engage communities that are uncertain or neutral on government use of AI.
- Deliberately analyze perceptions of benefits and risks of AI from each stakeholder group's point of view.
- When choosing how to implement an AI technology, focus on applications and safeguards rather than on the type of technology.
- Consider which data sources underpin AI technologies.
- Build trust in DHS and the broader U.S. government through continued partnerships.
- Consider partisanship's impact on DHS use of AI.
- Use multiple methods to routinely engage key stakeholders.
- Integrate public perception into technology development and acquisition life cycles.
- Ensure that public-perception studies are timely.

Contents

CHAPTER 5

APPENDIXES

Figures and Tables

Figures

Tables

CHAPTER 1

Introduction

Artificial intelligence (AI) systems, such as those that can recognize human faces or assess the likelihood that an event might occur, could be crucial in supporting the U.S. Department of Homeland Security's (DHS's) core missions. AI technologies have developed rapidly over the past decade, spurred by more-efficient computing power, large datasets, and novel machine learning models and approaches.[1] DHS already uses AI in homeland security missions, such as in border and airport security and with criminal investigations, and it is actively seeking to further integrate emerging AI capabilities into other applications across DHS components.

However, DHS's ability to use emerging technologies, such as AI, to their full potential is subject to several constraints, one of which is how the public views government use of those technologies. Public perception of government use of technology is important for several reasons, including the ability of government agencies (e.g., DHS) to establish trust in and legitimacy of its efforts, to facilitate necessary funding and legislative support from Congress, and to foster collaboration with technology companies and operational partners (Boudreaux, Yeung, and Steratore, 2022).

The U.S. government has experienced challenges to its implementation of some technology-oriented programs and has had to curtail these programs because of public outcry. For example, in 2009, DHS deployed a set of automated scanners at airports that displayed an image of a screened traveler's body to Transportation Security Administration (TSA) agents to help them detect threats. However, a wave of media reports and public criticism about the scanners' presentation of detailed full-body images drew attention to risks of privacy violation and discrimination (Stellin, 2010). Ultimately, DHS was pressured to remove hundreds of scanners that had already been deployed, thereby creating both financial and reputational costs for DHS (Ahlers, 2013).

More-recent examples further illustrate the role of public perception in leading to changes in technology programs throughout the government. In early 2022, after widespread public concerns were expressed about privacy risks, the Internal Revenue Service had to shelve plans to require the use of AI-based face recognition technology (FRT) for identifying taxpayers

[1] According to the DHS AI strategy, *AI* refers to "automated, machine-based technologies with at least some capacity for self-governance that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments" (DHS, 2020).

AI is also often defined as the ability of a computer to do things normally associated with human intelligence.

to enable them to manage their taxes online (Internal Revenue Service, 2022). Also in 2022, DHS rolled back its establishment of the Disinformation Governance Board (focused on social media–based disinformation campaigns) after heavy pushback from the media and members of Congress; some prominent legislators claimed that the board sounded like an Orwellian Ministry of Truth (Myers and Kanno-Youngs, 2022).

These examples of technology deployments illustrate the power of public perceptions to shape the government's ability to employ advanced technology programs—and the costs of ignoring what the public thinks. If the government does not take steps to solicit and ensure public support, future implementations of emerging AI technologies could have similar costly outcomes.

Various stakeholders—including members of Congress, state and local government officials, leaders of technology companies, and advocacy groups—have raised concerns about current DHS uses of AI. They contend that some DHS AI applications violate privacy and civil liberties, contribute to inequity, and are not subject to sufficient oversight or accountability that would ensure responsible use. These stakeholder groups have sought to marshal public pressure for the government to shape DHS use of AI, and their support is necessary for DHS to move forward with its AI goals. For instance, Congress can affect DHS use of AI and relevant programs through legislation or by restricting funding. Technology companies are essential partners for building the technological tools that DHS seeks to use, but some technology companies have vowed not to work with the government on some technology areas, including face recognition, until stringent regulations are in place and the public is more supportive. These companies seem to be responding to public perceptions of their association with government use of technologies that the public opposes or believes need stronger regulation. Other stakeholders can also influence whether DHS can effectively use AI. Figure 1.1 further illustrates the relationships among these key stakeholders and between the stakeholders and DHS use of AI technologies.

DHS itself has noted the importance of securing public trust and support for its use of AI, particularly in the DHS AI strategy:

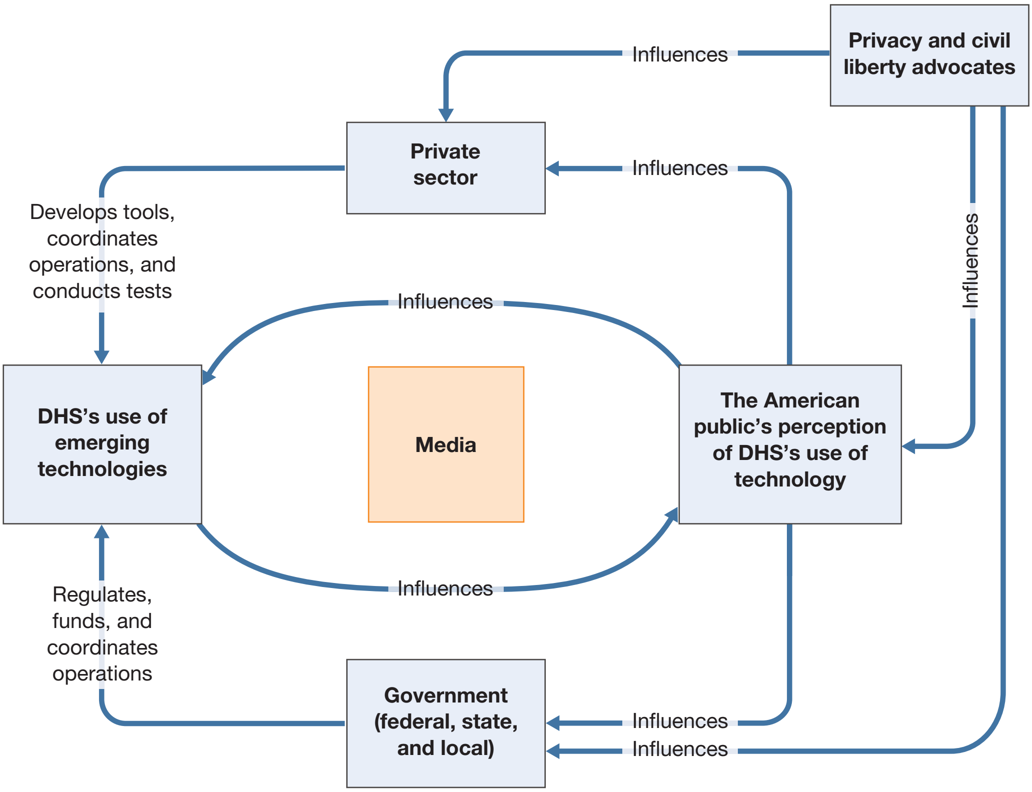
> Trust in the Department's expertise to identify and mitigate security risks and in its responsible use of its own AI systems is at the core of DHS's future success and leadership in AI. Furthermore, public input, especially in those instances where AI uses sensitive personal information, will improve the Department's accountability and increase the trust and confidence of the American people. (DHS, 2020, p. 1)

Here DHS has noted the importance of engaging the public to provide input in a way that will increase accountability and trust in sensitive AI applications. The DHS AI strategy also articulates, as one of the department's five major goals, that DHS will work to "improve public trust and engagement."

Achieving public trust requires that DHS understand the complex array of public perspectives across diverse communities in the United States to ensure that it can identify perceived benefits and concerns, and then to integrate those views to take steps to ensure the benefits

FIGURE 1.1

How Public Perception Could Influence Department of Homeland Security Use of Emerging Technologies, Such as Artificial Intelligence


Privacy and civil liberty advocates
Influences
Private sector
Influences
Influences
Develops tools, coordinates operations, and conducts tests
Influences
DHS's use of emerging technologies
Media
The American public's perception of DHS's use of technology
Influences
Regulates, funds, and coordinates operations
Government (federal, state, and local)
Influences
Influences

SOURCE: Adapted from Boudreaux, Yeung, and Steratore, 2022, p. 6.

while mitigating against risk. Understanding how the public perceives these technologies, and then designing and deploying them in a manner responsive to the public's concerns, is critical in gaining public support for DHS's use.

Given this context, we focused on gauging two broad aspects of public perception of AI: trust in government use of AI and support for specific uses of AI. For example, the degree to which the public trusts DHS to use AI could differ from its trust in the broader U.S. government's use of AI or the use of that technology in nongovernment contexts. The public might also more strongly support certain uses of AI, such as to identify victims of child sexual exploitation, than other uses. Or the public might support some AI technologies, such as face recognition, more than it supports others. In any of these cases, public trust and support might vary by demographic characteristics or prior experience with these technologies. With more-nuanced insight into the American public's views on these intertwined issues, DHS might better understand how to deploy and publicly message AI and other emerging technologies in ways that would help the department fulfill its missions.

The Purpose of This Study

There are many ways to explore public perception around DHS use of AI technology. This study employed one important approach: a survey that provides quantitative information about the public's perspectives of DHS use of AI across a diverse, nationally representative set of demographic groups. Understanding public perceptions of emerging technology is critical to acquiring, fielding, and supporting technology that the public is likely to accept and adopt. The aim of the study was to acquire quantitative information that would translate to guidance for acquiring and using these technologies in ways that the public would understand and support.

The overarching research questions we addressed in this study, developed in consultation with DHS, were the following:

- What are DHS components' current and planned uses of AI?
- What is the U.S. public's perception of DHS components' use of these technologies?
- What recommendations do public perceptions suggest for the effective and trustworthy use of these technologies?

To answer these questions, we interviewed DHS officials to understand their current and planned uses of AI, reviewed literature about AI technology and stakeholder perspectives on its uses, and developed and fielded a nationally representative survey of the American public.

Organization of This Report

In Chapter 2 of this report, we describe DHS uses of AI, including descriptions of several use cases that we prioritized in the public survey. Chapter 2 also provides information on concerns raised by key stakeholders, including members of Congress, civil liberty advocates, and technology companies, regarding DHS use of AI, such as risks related to privacy, equity, consent, and oversight. These concerns were included in the public survey to evaluate the extent to which the public shares them. Chapter 2 also provides a short description of other public surveys that informed the development of our own.

In Chapter 3, we provide background on the development of the survey, including the process we used to test the comprehensibility of the survey and the two-year delay in fielding the survey caused by required compliance with the Paperwork Reduction Act (PRA). In Chapter 4, we describe the findings from the survey, including high-level takeaways. Finally, in Chapter 5, we summarize the main findings and recommendations from this work.

In Appendix A, we provide the full survey instrument, including introductory and explanatory text, survey questions, and response options. In Appendix B, we describe the analytic approach to interpreting the survey results.

CHAPTER 2

Uses of Artificial Intelligence in Homeland Security

In this chapter, we present examples of the AI technologies that DHS is using to further its homeland security missions, and we describe key stakeholders' perspectives about risks of those DHS applications. The discussion of DHS uses of AI and stakeholder perspectives is not intended to be comprehensive across all technology applications and potential concerns; rather, we describe several DHS use cases that were prominent in 2020 while we were conducting initial research for the survey and some key stakeholder perspectives to provide background on the selected set of issues prioritized for survey inclusion.

Examples of Artificial Intelligence Technologies

With increased access to computing power and training data, along with new machine learning models and approaches, AI has developed rapidly in the past decade. DHS, like many federal agencies and nongovernmental organizations, sees opportunities to leverage AI to further its objectives (DHS, 2020). AI has had success in many areas related to DHS homeland security missions, such as object recognition, image and video generation, and language processing. We focus on four types of technologies that broadly fit the definition of AI: FRT, license plate–reader (LPR) technology, mobile phone location data, and risk-prediction technologies. Later in this chapter, a table summarizes many of DHS's most-common uses of AI technologies.

Face Recognition Technology

FRT is a type of biometric identification (fingerprinting is another that is better known) that uses an image of a face to verify or determine a person's identity. Unlike fingerprints and other types of biometric identification, FRT can be quickly used at a distance and at scale, leveraging algorithmic analysis of photos and videos to recognize faces. FRTs can take various forms. In one-to-one face recognition, FRT uses algorithms to compare the image of a face in a photo or a video to another source image—an authoritative, verified image—of a face (for instance, from a passport or driver's license photo) to verify whether the face in the new image matches the face from the authoritative image.

In one-to-many identification, FRT uses algorithms to compare the live image of a face to an images in an existing database or gallery to determine the identity of the face in the live image. The databases of labeled facial images used in one-to-many identification are available from multiple sources. For example, they can be purchased from commercial FRT vendors, some of which develop these databases from scraping facial images from social media and the broader internet. Government agencies can also seek access to existing databases administered by state and local law enforcement agencies, state and local departments of motor vehicles, U.S. Department of State visa and passport databases, and other sources (U.S. Immigration and Customs Enforcement [ICE], 2020).

Other forms of FRT include the use of algorithms to analyze an image of a face to determine the face's affective or emotional state (affect recognition). This might be used, for instance, to try to detect deception or whether someone seems likely to commit a crime.[1] FRT can also be used to count the number of faces (or people) in an image, assess someone's demographic features (such as gender, age, or race), or even try to identify what someone is doing.

License Plate–Reader Technology

Automated license plate or tag readers use high-speed cameras and algorithms to analyze images of license plates captured from surveillance video to determine details about vehicles. Data associated with a license plate (such as the plate number; vehicle make and model; state of registration; and the location, date, and time of capture) are also captured. This information can be used to match a license plate image to information about a vehicle's registration from department of motor vehicle databases. LPRs can also capture the surroundings in the image, which could include people in the vehicle. This technology can be used to determine the location of an automobile, track its movements, or identify its owner.

Mobile Phone Location Data

Mobile phone location data are collected by mobile phone applications and typically include Global Positioning System (GPS), Wi-Fi, or Bluetooth information that can pinpoint the device's location at various degrees of fidelity. Information about a device's location can be used to infer the location of the device's owner. Location data are available from commercial vendors for purchase on the open market, and these datasets might be used by government agencies for so-called *geofencing* to identify the people who were at a specific location and period, such as during a criminal activity, a riot, or a border crossing. Law enforcement might also get access to these or other types of location data from technology companies through court-administered subpoenas.

[1] DHS has funded and tested this sort of technology but has not deployed it (Daniels, 2018; Gershgorn, 2020).

Risk Technologies

Risk technologies are a broad class of AI systems that use algorithms and data to analyze how likely something is to occur, such as whether a shipment contains illegal goods, a person will commit a crime, or a hurricane will create a need for emergency responders. A variety of databases might be leveraged to develop these risk-assessment algorithms, including commercially available databases (such as credit card purchases), criminal records, public online activities (such as social media postings), and other open and proprietary sources.

Department of Homeland Security Uses of Artificial Intelligence

DHS has integrated these AI technologies across a variety of mission sets. We briefly review a few use cases that we judged were important for the public survey. We define *use case* as a DHS use of a particular technology in a specific application. By this definition, neither FRT alone nor the task of checking travel documents for air travel security it itself a use case, but the use of FRT to check travel documents for air travel security is a use case. Our discussion is not intended as a comprehensive overview of all DHS uses of AI or other technology but as a set of illustrative examples of potential importance to the public at large.

Airport and Border Security

Face Recognition Technology

DHS components, including TSA and U.S. Customs and Border Protection (CBP), have used FRT at airports and border crossings for more than a decade to verify travelers' identities. CBP uses FRT at airports across the country for verification of identities as travelers arrive into and depart from the United States (U.S. Government Accountability Office [GAO], 2022). And CBP manages the popular opt-in Global Entry program in which a U.S. traveler allows the use of FRT to expedite their clearance for international arrivals (CBP, 2023). According to CBP, automating the identity verification process with FRT promotes several important benefits: First, it "simplifies inspection and reduces impostor threats" by offering a more convenient and secure form of identity verification than manual human verification. Second, it "requires no direct contact and reduces the spread of germs," the benefit of which was realized (or amplified) during the coronavirus disease 2019 (COVID-19) pandemic. Third, CBP asserts that, because FRT reduces the labor burden on CBP staff, it "allows CBP officers to focus more on traveler safety." CBP argues that FRT "confirms traveler identity with more accuracy, security, and efficiency than ever before" and that the use of FRT has prevented more than 1,600 impostors from entering the United States (DHS, undated).

TSA is also testing the use of FRT at a sampling of U.S. airports in place of the standard manual security check by a TSA agent to verify passengers' identities as they board planes (Fowler, 2022; TSA, 2022a). TSA, like CBP, has stated that the use of FRT could provide better security and greater traveler convenience than manual screenings by agents can and that this allows TSA's human agents to focus on other important tasks (Fowler, 2022).

Risk-Assessment Technologies

TSA also has developed risk-assessment algorithms to detect threats related to passengers and baggage. These algorithms would rely on varied data to assess the probability of a threat and issue an alert for a TSA agent to conduct a manual screening. TSA officials have stated that these machine learning algorithms will "not only improve security effectiveness but also . . . will improve passenger experience through increased throughput and decreased false alarm rates" (TSA, 2020, p. 25). Risk-assessment algorithms could enhance travel security by leveraging data to determine threats, which would allow agents to prioritize the highest threats and thereby improve security and speed up screenings for other travelers.

CBP uses the Automated Targeting System to score the risk of travelers crossing the U.S. border "for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the US" (DHS, 2010). It does so by comparing traveler, cargo, and conveyance information against data from at least 25 government databases, including those of law enforcement and intelligence agencies (Electronic Privacy Information Center, 2019). This system creates the criteria for flagging material and people by recognizing patterns established by CBP officer experiences, suspicious-activity trends, intelligence, and law enforcement considerations.

License Plate Readers

DHS also uses LPRs as part of its suite of surveillance systems to provide situational awareness and to support law enforcement efforts. This technology aids in the detection, identification, and apprehension of people suspected of being involved in illegal activities (Science and Technology Directorate [S&T], 2021a). CBP also uses LPR data to identify targets involved in illegal activities across borders, including those abetting movement of terrorists, weapons, and narcotics.

Government Facility Security

The U.S. Secret Service (USSS) has tested and piloted the use of FRT to assist with the identification of known subjects of interest around the White House (USSS, 2018). Although USSS has not enacted this program, FRT could also be used in place of existing identity verification tools for further integration in facility security applications (similarly to how FRT is used in airport and border security) for entering government facilities.

Immigration Enforcement

ICE uses FRT and LPRs to determine whether someone in the United States possesses proper documentation to be in the country (Ng, 2019; Talla, 2019; Wang et al., 2022). ICE has contracts with the controversial company Clearview AI (giving the company access to tools that use a web-scraped database of labeled faces) (Lyons, 2020), and ICE can access state driver's license photo databases, enabling broad face recognition capabilities to support immigration enforcement goals (Harwell, 2019c).

There are also reports that ICE and CBP have purchased mobile phone–based geolocation data to track the flow of people across the border (Aleaziz and Haskins, 2020; Cox, 2020; Tau and Hackman, 2020). Mobile phone data sources have been used to identify people who might have entered the United States without authorization, and these data might also help these agencies patrol specific border areas in remote locations or in tunnels where migrants are crossing.

Criminal Investigations

According to a June 2021 GAO report, 20 U.S. government agencies, including four DHS components (CBP, ICE, TSA, and USSS), use FRT to support investigations of suspected criminal activity. The protests following the murder of George Floyd and images taken during the January 6 insurgency at the U.S. Capitol are two examples of federal use of FRT (GAO, 2021).

ICE's Homeland Security Investigations (HSI) also uses FRT "to identify victims of child exploitation and human trafficking, subjects engaged in the online and sexual exploitation of children, subjects engaged in financial fraud schemes [or] identity and benefit fraud, and those identified as members of transnational criminal organizations" (ICE, 2020, p. 6). There are many reasons HSI would want to identify someone. The mere fact of a person exiting an area of interest might not be sufficient to generate an arrest warrant, but it could be useful for HSI to identify that person nonetheless: They might have an active arrest warrant, they might be a known or suspected part of a criminal network, or they might just be noted in case they appear elsewhere. In this case, a substantial advantage of face recognition is that it is a form of identification that does not alert the suspect and can be used at a distance.

In addition, LPRs and mobile phone location data are used for supporting criminal investigations and might be used in tandem with FRT to develop a more holistic and accurate identification of a person of interest.

Victim Identification

FRT can also be used to identify crime victims from a victim's facial images. For instance, HSI uses FRT to identify victims of child exploitation and sexual abuse by matching images from sexual abuse material to HSI's internal victim database (ICE, 2020).

Incident Prevention and Preparedness

DHS uses technologies that assess the risk of an event to prepare and pre-position resources for both naturally occurring and human-caused incidents. Risk technologies also can be used to target screenings for shipments or bags to prevent security incidents or other harms. DHS has also invested in social media analytical toolkits that aggregate social media activity (e.g., tweets) to assist first responders in gaining situational awareness that is useful for emergency preparedness and response (Marullo et al., 2020).

Other Possible Department of Homeland Security Uses

There are other possible applications of AI technologies that DHS is not currently or planning on using but that might relate closely enough to DHS homeland security missions that their potential use warrants inclusion in our assessment. These include the use of FRT or other identity verification technology at voting locations to ensure the integrity and credibility of elections, the use of FRT or other identity verification at nonfederal buildings for security goals (such as schools, sports stadiums, or other places with security risks), the use of FRT (in particular, affect recognition) to detect whether someone is likely to commit a crime, and the use of FRT along with risk-assessment technologies to determine whether a person of interest is lying about their immigration status. Table 2.1 lists DHS use cases for a variety of AI technologies.

TABLE 2.1

Artificial Intelligence Technologies and Department of Homeland Security Use Cases

	FRT				
DHS Use Case	**One to One**	**One to Many**	**Risk Technology**	**GPS Location Tracking**	**LPRs**
Airport and border security	x	x	x		
Government facility security	x	x	x		
Identifying a victim		x			
Identifying a suspect or person of interest		x		x	
Predicting the likelihood of an event			x		
Predicting who will carry out an attack			x		
Incident prevention and preparedness			x		
Immigration enforcement				x	x
Criminal investigation					x

Public Stakeholder Concerns About Uses of Artificial Intelligence

Various stakeholders—including members of Congress from all political parties (Konkel, 2021), state and local government officials, technology companies (Hao, 2020; Peters, 2020), and civil society groups (Access Now et al., 2021; Center for Democracy and Technology, 2021)—have expressed significant concerns about DHS uses of these technologies. As discussed in Chapter 1, these concerns are important in that they could affect DHS's ability to use AI technologies. The concerns raised by stakeholders already have led to U.S. municipalities and international partners banning or restricting the use of AI technologies, including FRT (Halter, 2021; Harwell, 2019a; McKay, 2020; Pollina and Maccioni, 2022). These concerns have also led technology companies to declare a moratorium on the sale of FRTs to the federal government until Congress passes legislation that serves as effective guardrails (Hao, 2020; Hill and Mac, 2021; Peters, 2020). Members of Congress also have raised a variety of concerns and have sought to restrict or regulate DHS use of AI technologies. The public debate around these concerns also might foster mistrust in ways that undermine public support or acceptance of DHS applications.

In this section, we briefly describe some key concerns raised by these stakeholders. There is not a monolithic view about DHS use of these technologies, and different stakeholders emphasize different concerns or evaluate the benefits and risks differently. The concerns on which we focus here were included in the public survey to evaluate the extent to which they were shared among the public and whether the public believes that the benefits of DHS use of AI might outweigh these concerns.

Privacy

Stakeholders—including members of Congress, civil liberty organizations, and technology companies—have noted the risks that AI-enabled government surveillance poses to privacy and civil liberties. FRT, mobile phone location data, and other AI technologies provide a powerful set of tools to identify and locate a person across places and times. As DHS and other government agencies use these tools more widely in homeland security and other contexts, the government has rapidly expanded its ability to identify people in ways that might be easily abused (Harwell, 2019b; Rudolph, Moy, and Bedoya, 2017). Government surveillance has also become more widespread and encompassing as it leverages different technologies across contexts—by, for instance, combining FRT with mobile phone location data or social media postings for a more comprehensive approach to identify people. Members of Congress and advocates have argued that this ability creates a surveillance "dragnet" that can also reveal highly private information, such as "where we sleep at night, where we go to the doctor, who we spend time with, and every other aspect of our lives" (Aleaziz and Haskins, 2020, quoting Nathan Freed Wessler, an attorney with the American Civil Liberties Union [ACLU]; see also Wang et al., 2022).

LPR technologies are also subject to these criticisms. For instance, the ACLU contends that this technology is "deployed with too few rules [and] is becoming a tool for mass routine location tracking and surveillance" (ACLU, undated).

Advocates have noted that the widespread use of these AI technologies can result in fewer or no opportunities for anonymity or privacy in public in a way that is detrimental to individuals' civil liberties. The use of these tools can also interfere with people's ability to exercise their First Amendment rights to express themselves freely—for instance, they might create a fear among the population that discourages them to peacefully protest or associate with whom they choose. These stakeholders have argued that the government must proceed very cautiously with these technologies to ensure that infringements on privacy are explicitly legally authorized and can be publicly accountable to ensure that there is not overreach or abuse.[2]

Equity

A large volume of academic research has shed light on the inequities associated with the use of emerging AI technologies, and stakeholders have noted that the risk of perpetuating or exacerbating inequity is a major concern about DHS technology applications. Indeed, the Biden White House itself has stated, "There is extensive evidence showing that automated systems can produce inequitable outcomes and amplify existing inequity" (Office of Science and Technology Policy, undated). AI technologies, such as FRT, are trained on datasets that are not representative of American society, and the biases within these datasets (combined with the inherent blind spots of a relatively homogeneous group of AI developers) have resulted in systems that are often not equally accurate across all demographics (Buolamwini and Gebru, 2018). Thus, the use of these technologies might have a disparate impact on marginalized communities, such as Black Americans and other people of color.

In 2019, the National Institute of Standards and Technology tested the accuracy of FRT across demographic groups and found that some FRT algorithms' performance varies significantly based on demographic characteristics (Grother, Ngan, and Hanaoka, 2019). For instance, some FRTs perform significantly worse against Black and Asian people than against White men. These disparate error rates can result in Black people and other minorities being subject to increased false positives in one-to-many identification, which, in turn, could lead to a greater likelihood of their being wrongfully accused of criminal or other conduct than if they were White. Indeed, there are already multiple reported examples of wrongful arrest of Black men due to errors with FRT (Hill, 2020a; Hill, 2020b; Johnson, 2022). Insofar as these systems contain inaccuracies, the burdens of these errors will fall disproportionately on those

[2] DHS and other government agencies are subject to legal requirements when they collect personally identifiable information (PII), including the Privacy Act of 1974 (Pub. L. 93-579). Even with compliance with existing law, stakeholders have argued that these new technologies still infringe on personal privacy.

who are already marginalized. Thus, the use of AI technologies by government agencies perpetuates harmful inequity across American society.

Stakeholders have argued that, even if AI technologies can become perfectly accurate or at least equally accurate across demographic groups, the use of these technologies might still contribute to inequity. In particular, the harmful privacy implications from a potentially more widespread surveillance state are particularly problematic for people of color and other historically marginalized populations. These communities already face inequitable policing and surveillance, and more-powerful technologies might be used or abused in ways that target minorities for punitive actions (Center for Democracy and Technology, 2021). The chilling effects on free expression and free association might also be more pronounced for these communities, discouraging them from protesting or otherwise calling attention to systemic inequity. So even when AI technologies are accurate, they might be harmful to civil rights or used for abuse in inequitable ways.

In addition to FRT, risk assessment is another technology known to reflect and produce inequity. Studies have shown that these technologies result in different error rates across demographic groups that, for example, wrongfully identify a Black person as higher risk of criminality than a White person (see references in Office of Science and Technology Policy, undated). If historical datasets reflect a biased view of criminality or of other areas of risk, then risk-assessment algorithms will inherit and promulgate these biases. This can have detrimental consequences to those who are wrongfully deemed high risk and might increase mistrust between DHS and communities of color that already feel targeted by inequitable law enforcement practices.

LPRs might also be used or misused in inequitable ways. In one example of misuse, the Oakland (California) Police Department disproportionately deployed automated LPR cameras in low-income communities and communities of color. The technology can also be misused by individuals. For example, a Washington, D.C., police officer used LPR to search the plates of vehicles near a gay bar and blackmailed the vehicle owners (Electronic Frontier Foundation, 2017).

Oversight

AI technologies have advanced rapidly in the past decade, and the development and application of these tools have also grown rapidly, with very limited new federal legislation or other regulations that guide government use. A large market of private data brokers selling mobile phone location information has sprouted, and the U.S. government can now purchase from vendors information about a person's whereabouts that otherwise would not have been available or available only under court-administered legal subpoenas. Several members of Congress have raised concerns about DHS purchase of geolocation data in the absence of federal authorization and have noted their suspicions that the practice violates Fourth Amendment constitutional protections (Cox, 2020).

In addition, U.S. government agencies, including DHS, contract with FRT companies, such as Clearview AI, despite those companies being under significant legal and public scrutiny both in the United States and abroad for their data-harvesting practices (Heikkilä, 2022; Rodrigo, 2021). Civil liberty advocates have coalesced to pressure DHS to cease using Clearview AI (Rodrigo, 2021). There are currently no explicit legal prohibitions or requirements on DHS to refrain from contracting with these commercial vendors.[3] And according to GAO, many federal agencies do not even have systems in place to track which nonfederal systems employees use (GAO, 2021, p. 22). For instance, USSS reported that it does not track what information systems are being used (GAO, 2021, p. 22).

Stakeholders have noted that, in the absence of new policies and processes, oversight of how DHS is using these technologies is insufficient. No federal, state, or municipal laws require auditing of the proprietary and black-box algorithms DHS uses. These stakeholders have argued that, without explicit congressional authorization and opportunity for external audits, DHS use of AI tools should be limited (Rudolph, Moy, and Bedoya, 2017).

Proper Notice

Stakeholders have raised an additional and related concern regarding the type of notice and information that DHS provides to Americans regarding its use of AI technologies. Many people in the United States might be unaware of how and when DHS uses FRT and other technologies at border crossings, airports, or other contexts. For instance, according to GAO, "CBP had not consistently provided travelers with information about FRT locations" (GAO, 2022). Similarly, little information is provided to the public about which databases are used in FRT identification or when and how DHS might be using LPR technologies.[4] The information that is provided tends to be contained in general reports (such as privacy impact assessments) rather than within specific and explicit notices each time the technology is being used.[5]

According to stakeholders, such as civil liberty advocates, providing proper notice to Americans regarding DHS uses of technology is required by constitutionally protected due-process rights and is a fundamental component of procedural justice. These advocates argue that, without sufficient notification, Americans cannot make informed decisions or have

[3] However, government agencies, including DHS, must comply with the Privacy Act of 1974 (Pub. L. 93-579) provisions pertaining to the collection of PII.

[4] According to the ACLU, for example,

> Records obtained by the ACLU of Northern California in a Freedom of Information Act lawsuit detail ICE's sweeping use of a vast automated license plate reader (ALPR) database run by a company called Vigilant Solutions. Over 9,000 ICE officers have gained access to the Vigilant system under a $6.1 million contract that the public first learned of last year. ICE has access to over 5 billion data points of location information collected by private businesses, like insurance companies and parking lots, and can gain access to an additional 1.5 billion records collected by law enforcement agencies. (Talla, 2019)

[5] And the privacy impact assessments themselves note that there is a risk that the face recognition services "will not provide adequate notice that its biometric collections may be used for facial recognition matching" (ICE, 2020, p. 19).

transparency about how the government uses these technologies in ways that would ensure accountability and legitimacy (Center for Democracy and Technology, 2021).

It is noteworthy that some state and local laws (such as New York City's biometric privacy law) require that entities that use FRT or other biometric surveillance provide formal notice that they are collecting data (N.Y.C. Admin. Code, Title 22). However, there is no comparable federal law that would apply to DHS.

Lack of Consent

A related issue to proper notice concerns whether and how individuals can affirm or deny their consent regarding the use of these technologies. Some advocacy groups have noted that, for some technology deployments, such as FRT, no reasonable opportunities exist to opt out. This relates both to photos that are used in FRT databases and to how these technologies are used.

DHS components, such as TSA, have noted that they strive to provide opportunities to opt out of these use cases: "Travelers who do not wish to participate in the facial matching process can opt out in favor of an alternative identity verification process" (TSA, 2022b). However, according to some advocates, "What we often see with these biometric programs is they are only optional in the introductory phases—and over time we see them becoming standardized and nationalized and eventually compulsory" (Fowler, 2022). If opting out of a technology requires an arduous or inconvenient process, this means that the technology becomes a de facto requirement (Sankin, 2020). In addition, whether someone can actually opt out depends on there being clear information about how to do so, and, according to GAO, "CBP's privacy signage provided limited information on how travelers could request to opt out of FRT screening and were not always posted" (GAO, 2022).

As with providing proper notice, several state and local biometric privacy laws (such as in Illinois and Texas) require that individuals consent to the collection of their biometric data, such as images of their faces. However, there is no comparable federal law that applies to DHS use of FRT.

Cybersecurity and Data Management

A final concern relates to the data management practices surrounding the sensitive information collected and processed by AI technologies. PII, such as a person's face, is highly sensitive and, if accessed by a malicious actor, could be used in criminal and other harmful ways. In some ways, this information might be even more sensitive than traditional passwords because, unlike a password, someone's face cannot be readily changed, so the use of facial images might pose a security threat for someone's entire life. The U.S. government has suffered several high-profile data breaches, including a breach of Office of Personnel Management data that exposed sensitive information, such as social security numbers, of millions of Americans (U.S. Office of Personnel Management, undated), and DHS itself has also been hacked (Miller, 2020). The more information that the government collects, the more valuable a target it becomes for hackers. Thus, it is extremely important that the U.S. government develop more-robust cybersecurity and data management practices than it has displayed to date.

Additional questions concern how data collected by or used in AI technologies are shared with other entities, including other law enforcement entities in the United States or other operational partners.

Potential Safeguards on Department of Homeland Security Uses of Artificial Intelligence

The concerns just discussed helped us identify a set of potential safeguards that might improve public perceptions of AI use by DHS, such as the following:

- allowing people to opt out of FRT or other technology
- requiring regular external audits by credible and independent parties to ensure accuracy and equity
- mandating destruction of images or other data when they are no longer needed
- requiring court orders before using AI in certain contexts
- requiring consent from people before images of their faces are collected or shared
- requiring that more information be provided about the purpose of the AI application, how DHS will use it, and DHS's privacy policies
- requiring special training for agents who use AI
- securely storing images and other data.

These considerations were included in the survey to explore whether the public believes that these potential safeguards would assist DHS in maximizing the benefits of AI while mitigating concerns.

Existing Surveys Relevant to Department of Homeland Security Use of Artificial Intelligence

Some existing surveys related to DHS use of AI were informative for shaping our own. For example, the Pew Research Center has conducted a series of surveys using the center's American Trends Panel (Pew Research Center, undated), an online survey panel recruited through random sampling of U.S. home addresses. Gender, race, ethnicity, political ideology, education, and other categorical weights are applied to survey responses to ensure representation of the U.S. adult population. Using this panel, researchers have assessed public attitudes on a variety of science and technology topics, including safety of genetically modified foods and vaccines, access to experimental treatments, climate change, and AI and human enhancement (such as genetic modification) (e.g., Pew Research Center, 2015a; Rainie et al., 2022).

Emerging science and technology issues often generate mixed public reactions (Funk, 2020), including views on the U.S. federal government's role in addressing these issues. For example, a recent decrease in support for government regulation of technology companies has emerged, particularly among Republicans (Vogels, 2022), while some other topics, such as climate change, are more generally thought to have too little federal action (Tyson and Kennedy, 2020).

The findings of a recent Pew survey that assessed public views on AI and human enhancement technologies (Rainie et al., 2022) align with findings from other Pew surveys that found a wide set of drivers of public opinion on AI. These drivers include a combination of individual-level factors—such as political ideology, age, education, gender, race and ethnicity, and religion (Pew Research Center, 2015b; Vogels and Perrin, 2022)—as well as the technology deployer, intended user, end goals, and specific application. For instance, younger people are likelier than older people to say that they favor policies to address climate change but less likely to say that childhood vaccines should be required.

Academics are studying related topics, such as the influence of the COVID-19 pandemic on attitudes about AI-enabled autonomous systems (Horowitz et al., 2022), as well as a comparative study on public acceptance of FRT in China, Germany, the United Kingdom, and the United States (Kostka, Steinacker, and Meckel, 2021). Kostka and her coauthors argued that public acceptance of FRT is driven by sociodemographic factors and prior experience, as well as perceived benefits, risks, usefulness, and reliability of these technologies.

Despite these and other efforts, studies on public perspectives of the U.S. government's (specifically DHS's) use of FRT are limited. We aimed to help fill this gap to better understand public perspectives of DHS's use of FRT.

CHAPTER 3

Fielding a Nationally Representative Survey of Public Perceptions

This chapter provides background on the development and fielding of a nationally representative survey of public perceptions of DHS uses of AI and includes discussion of the two-year delay in fielding the survey due to required compliance with the PRA. The complete survey instrument is reproduced in Appendix A.

Survey Development

Background Research for Survey Content

To identify appropriate survey topics and questions, we first reviewed literature related to emerging AI technologies and stakeholder perspectives on these technologies. We also reviewed existing public surveys on technology and perspectives on government use of technology.

In addition to this literature review, we conducted a series of interviews facilitated by our S&T sponsor with DHS officials who had expertise on DHS uses of AI. These interviewees included representatives from S&T's Technology Centers who worked on the development and integration of technologies across DHS and S&T portfolio managers who worked with DHS components and provided information about how those components used AI. Because the interviews were for background purposes, we do not provide details here; however, they were important for identifying key DHS documents and viewpoints that we used to develop the survey.

Survey Drafting

We worked with our S&T sponsor to prioritize four AI technology areas to include in the survey: FRT, LPR technology, mobile phone location data, and risk-assessment technology. These technologies were subject to significant public discussion in 2020 while the survey was being developed. Working with our sponsor, we judged that DHS and broader U.S. government use of FRT was a priority for the public; thus, the survey devoted additional questions to exploring public perceptions of it. We drafted the survey with several guiding considerations, including the importance of limiting its length and ensuring that it would be broadly comprehensible at a seventh- or eighth-grade reading level to a diverse set of American respondents. We also included a mix of open- and closed-ended questions to provide respondents multiple opportunities to share their perspectives.

Survey Testing

We tested an initial draft of the survey through a set of nine one-hour cognitive interviews with a demographically diverse set of people selected with the assistance of the RAND American Life Panel (ALP) (more information on this panel is provided later in this chapter). These nine cognitive interviews were designed to elicit insight about whether the questions and response options would be interpreted as we intended, whether any questions would be difficult to understand, whether response options would be difficult to use, whether the order of questions made sense, and any additional suggestions the interviewee had to improve the survey. Informed by the cognitive interviews, we significantly revised the survey to improve its readability, reduce ambiguity, and ensure that the survey could be completed in a reasonable time.

We finalized the survey in March 2021. Using a timing algorithm and the insights from the cognitive interviews, we estimated that the survey would take 16 minutes to complete.

The Paperwork Reduction Act Process

Before fielding the survey, we needed to meet the procedural requirements of the PRA. The PRA is a federal law to reduce the paperwork burden that the U.S. government can impose.[1] Before a government agency can collect information from the public (generally defined as ten or more people who are not federal employees), it must satisfy a series of procedural requirements. Because our survey would involve collecting information on DHS's behalf from several thousand people, we were obligated to seek approval through the PRA process. The PRA's procedural requirements are managed by OMB, which must ultimately approve the information collection before it can be conducted.

The PRA requires the development of documents that describe the burden on the public that the information collection will create and that provide details on data management and privacy protections. In addition, the PRA requires a 60-day request for comment in the *Federal Register*, which requests public feedback on whether the information collection is necessary and on the accuracy of the estimate of the burden to the American public. Following review and consideration of public comments, the PRA requires a second 30-day notification in the *Federal Register* before it is submitted to OMB for approval.

[1] This section draws on "A Guide to the Paperwork Reduction Act" (U.S. General Services Administration and Office of Management and Budget [OMB], undated).

Public Comments from the Federal Register Request

The initial 60-day request for comment was posted in the *Federal Register* on May 13, 2021 (S&T, 2021b), and we received three public comments. The 30-day notification was posted in the *Federal Register* on November 5, 2021 (S&T, 2021c), and we received 219 comments. Most of these comments offered a perspective on the benefits and risks of DHS use of FRT and other AI technologies, as opposed to describing concerns about survey design or public burden. The substantive comments on benefits and burdens mirrored the types of considerations presented by stakeholders (discussed in Chapter 2), including such issues as privacy, equity, and oversight, and thus were the types of perceptions we sought to further evaluate within the public survey. Per the PRA process, we responded to each of these comments, emphasizing that, although the survey was about AI technologies, the survey itself would collect only survey data and would not collect any face recognition information or otherwise use AI. Our responses to these comments also clarified that the anonymous results of the survey would be shared with the public. These responses were completed on February 10, 2022.

On October 12, 2022, we received final approval from our DHS sponsor that necessary requirements had been met to field the survey.

Survey Fielding

We began fielding the survey on October 17, 2022. ALP participants received weekly reminders to complete the survey, and the survey closed on November 27, 2022, with 2,841 completes and a 79.9-percent completion rate.

The RAND American Life Panel

ALP is a nationally representative internet panel of American adults who speak English or Spanish (Pollard and Baird, 2017). ALP uses computer-assisted web interviewing programming software that allowed the survey to be administered across several types of hardware platforms, such as desktop and laptop computers, smartphones and other mobile phones, and tablets. The survey was accessible across operating systems as well. In addition, panel members who did not have internet access were provided with Chromebooks. This ensured that the survey could be completed by a diverse selection of respondents, including those without regular access to a computer or the internet.

ALP members are sent email invitations to participate in surveys and regularly receive reminders to complete invited surveys. Panel members are selected to take surveys on varying schedules about various topics.

Part of the reason we selected web-based interviewing as the means of collecting data was to minimize burden on respondents and to collect data in a cost-efficient manner. Study respondents submit their responses via computer, at a time and location of their choosing.

The collection of data was fully electronic—all information was completed on and submitted from a web form. In addition, data reliability was enhanced because study participants directly entered their responses, nullifying the risk that an interviewer would miscode what a participant actually said. Additionally, because respondents did not directly share their answers with an interviewer, they might have been likelier to answer truthfully.

All information was collected on a voluntary basis, and DHS did not receive any PII from the respondents.

Survey Limitations

Several factors could limit the generalizability of these survey findings or the extent to which they accurately capture public views. First, the survey content was finalized in 2020, based on a literature review and preliminary insights from cognitive interviews and discussions with DHS stakeholders.

The literature review was intended to generate insight about AI technologies used by DHS, the opportunities and limitations of those technologies, and stakeholder views of the benefits and risks. However, the literature review was not a comprehensive review of all aspects of AI or potential homeland security use cases; rather, we prioritized issues of particular interest to the DHS sponsor.

The interviews with DHS officials were semistructured, with six points of contact identified by our DHS sponsor. These DHS officials described their roles in integrating AI into homeland security missions, but we did not have access to any DHS-sensitive or other proprietary information. We also were able to interview only a small number of officials with experience with DHS AI deployments.

Because the survey was not fielded until two years after the literature review and interviews, there might be a mismatch between topics prioritized at that time and those that survey respondents considered important. Recent advances in AI technologies (e.g., tools based on generative AI, such as DALL-E and ChatGPT) and changes in DHS applications or policies (e.g., surrounding privacy protections) that have emerged since the survey was developed would also not be included in the survey.

Also notable was the degree to which the survey's topic area (government use of AI) appeared to have heightened interest, including some concerns, among prospective respondents. As mentioned earlier, we received more than 200 comments about the survey in the public comment period. Once the survey was fielded, several ALP members expressed concerns that completing the survey could adversely affect their employment, suggesting that they perceived the topic as sensitive. We responded to each such query by acknowledging that any survey that asks about sensitive issues could have a negative impact if an employer were to learn of a response through a breach of confidentiality. We then assured respondents that multiple steps were taken to ensure that responses were confidential and that no individual results would be made public, so there would be very little risk. We were unable to assess the extent to which these concerns affected survey results: Any ALP member who expressed concerns could still complete the survey, and we could not link them with their messages. However, overall nonresponse was low. The overall response rate was almost 80 percent of people who were contacted to complete the survey, which compares favorably with other ALP surveys of similar lengths. In the survey itself, nonresponse never exceeded 3 percent for an individual question.

A final and important limitation involves the political ideology or partisanship of the ALP respondents. We were unable to include political partisanship in the constructed survey data weights, which was weighted for other demographic characteristics. We included self-reported partisanship preferences as a model covariate in our statistical analysis. As discussed in Chapter 4, respondents reporting liberal or conservative ideologies seemed to have similar attitudes toward government use of AI technology to attitudes of centrist respondents. However, it is not clear how reweighting the survey to account for political ideology would affect the descriptive analyses.

CHAPTER 4

Survey Results: Public Perceptions of Department of Homeland Security Use of Artificial Intelligence

This chapter reports several analyses of public perceptions. First, we provide descriptive analyses of survey responses to identify Americans' overall concerns and views. We also further analyzed these responses to determine whether public perceptions were associated with any demographic differences. Finally, we explored whether different kinds of opinion (e.g., views on different types of technology) were related to one another. Appendix B provides additional details of the full analytic approach.

The survey findings and analysis focus more heavily on FRT than on other uses of AI. This was at the request of the sponsor and because FRT gets significant attention in the national discourse.

Summary of Survey Findings

These are the high-level findings from the survey, with further details presented in the rest of this chapter:

- Significant numbers of respondents might not have formed opinions about government use of FRT.
- Respondents reported agreement that the government's use of FRT had both benefits and risks, but they were likelier to acknowledge risks than benefits.
- Respondents reported that security, accuracy, and privacy than speed or convenience were more important for government use of FRT.
- Respondents reported agreement that the government's use of FRT raised multiple types of risk, including misuse, inaccuracy, and bias.
- Less than one-quarter of respondents reported trusting the government's use of FRT.
- Safeguards could improve the public's comfort with government use of FRT, but the overall effect might be limited.
- Respondents reported believing that government must meet certain requirements for using FRT.

- Public support depends more on the application than on the technology.
- Respondents reported supporting some government applications of FRT, such as criminal investigations, but not others, such as identifying people at protests or public spaces.
- Respondents' reported support for risk technologies varied by application and data source.
- Respondents' reported support for LPRs and mobile phone location data varied by government application.

Public Perceptions of Face Recognition Technology

Significant Numbers of Respondents Might Not Have Formed Opinions About Government Use of Face Recognition Technology

A large proportion of responders to questions about government use of FRT chose not to respond to questions about benefits and risks, responded "don't know/it depends," or responded in ways that suggested they were neutral about the government use.

On the 12 survey questions related to U.S. government use of FRT, 240 of the 2,841 respondents chose not to respond or responded "prefer not to say" at least once. The percentage of these nonresponses for the FRT questions never exceeded 3 percent of all responses for any question. However, beyond the "prefer not to say" response, for nine of the 12 FRT survey questions, respondents also had the option to indicate a neutral response ("neither agree nor disagree") or a response indicating ambiguity or no opinion ("don't know/it depends"). Across the survey questions, a significant number of respondents' answers were neutral or ambiguous (see Figure 4.1):

- 41 percent of respondents when asked whether FRT's benefits outweigh its risks
- 45 percent of respondents when asked whether U.S. government use of FRT's benefits outweigh its risks
- 36 percent of respondents when asked whether they trusted U.S. government use of FRT
- 35 percent of respondents when asked whether they trusted DHS use of FRT.

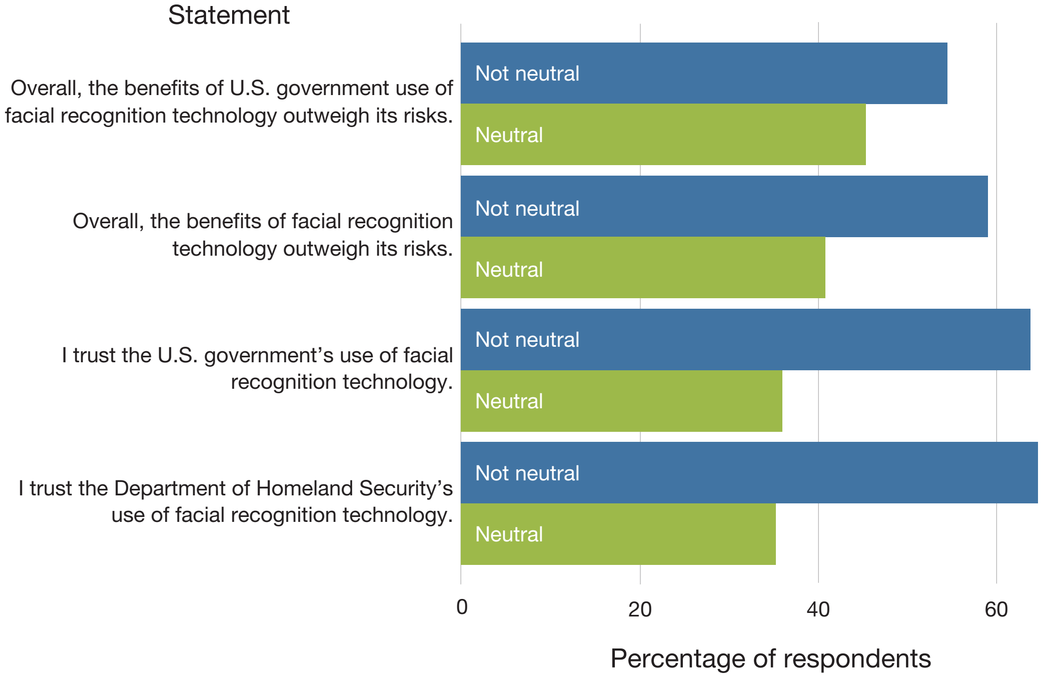
Neutral or ambiguous responses

- averaged 24 percent and ranged between 13 percent and 35 percent of respondents for 14 FRT applications
- averaged 17 percent and ranged between 10 percent and 28 percent of respondents for nine questions about requirements for U.S. government FRT use
- averaged 21 percent and ranged between 13 percent and 27 percent of respondents for six questions about photo source options for U.S. government FRT use.

We did not detect patterns of significant demographic association with these neutral and ambiguous responses; respondents across different ages, genders, races, and socioeconomic

FIGURE 4.1

Percentage of Respondents Who Reported Feeling Neutral or Ambiguous About Government Use of Face Recognition Technology



SOURCE: Features ALP data.

NOTE: Missing responses are excluded. *n* = 2,841 respondents.

statuses generally reported having these neutral or ambiguous attitudes. We did, however, observe that men were less likely than women to respond neutrally or ambiguously on 30 of the 87 subquestions with the option for a neutral or ambiguous response. Given the large number of respondents without strong opinions on government use of FRT, this suggests that there are opportunities for DHS to further survey, educate, and otherwise engage the public.

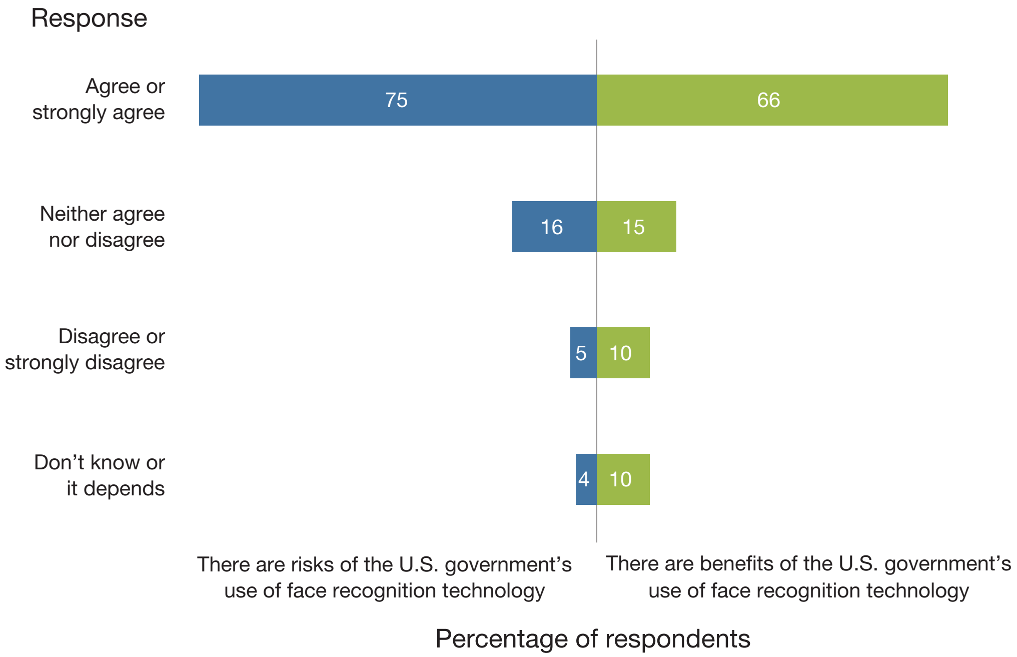
Respondents Reported Agreement That the Government's Use of Face Recognition Technology Had Both Benefits and Risks, but They Were Likelier to Acknowledge Risks Than Benefits

The majority of respondents reported agreeing that there were both benefits and risks of FRT in general, although more said that they agreed that there were risks (79 percent) than that there were benefits (73 percent). Only 38 percent reported agreement that the overall benefits of FRT outweighed its risks. However, 41 percent of respondents reported feeling either neutral or ambiguous about or did not answer this question, suggesting that the public's attitudes about the evaluation of benefits and risks are still somewhat unclear.

Comparing respondents' views of U.S. government use of FRT and their views on FRT use in general, fewer respondents reported perceiving benefits of government use of FRT than FRT use in general. The majority of respondents reported agreeing that there were both benefits and risks of the U.S. government's use of FRT (65 percent and 75 percent, respectively), while only 34 percent reported agreement that the overall benefits outweighed its risks. And a relatively large proportion of respondents (45 percent) provided answers that were either neutral or ambiguous or did not answer the question (see Figure 4.2).

FIGURE 4.2

The Public Perception of Benefits and Risks of Government Use of Face Recognition Technology



SOURCE: Features ALP data.

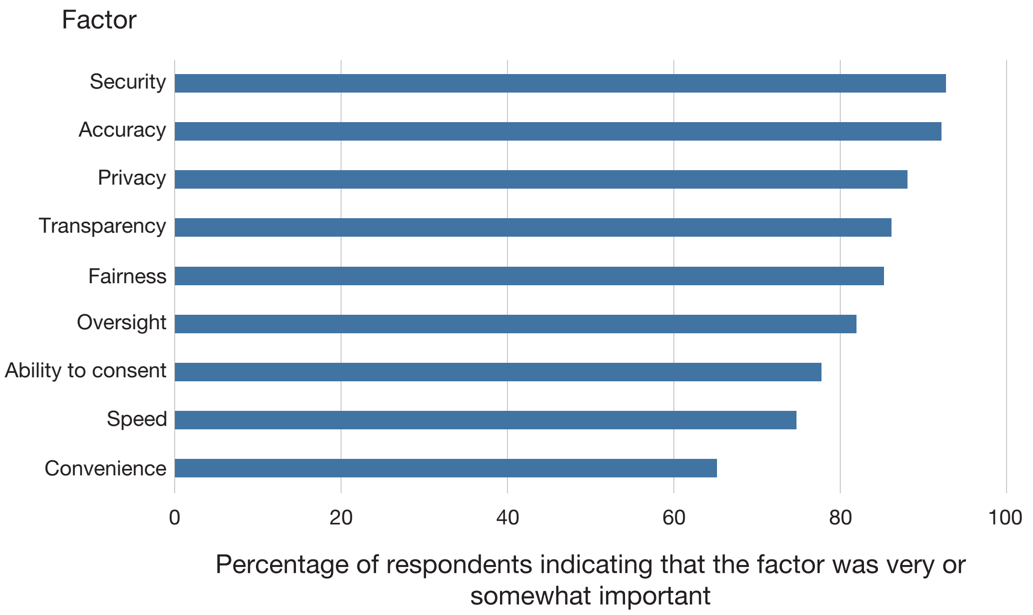
NOTE: Missing responses are excluded. *n* = 2,841 respondents.

The Public Sees Security, Accuracy, and Privacy as More Important Than Speed or Convenience for Government Use of Face Recognition Technology

Respondents were asked to rate the importance of several features of government use of FRT, and they generally reported agreement on the importance of a broad set of issues (see Figure 4.3). Respondents also generally reported agreement that security, accuracy, and privacy issues were more important than speed or convenience.

FIGURE 4.3

What Factors Are Important for Government Uses of Face Recognition Technology?



SOURCE: Features ALP data.

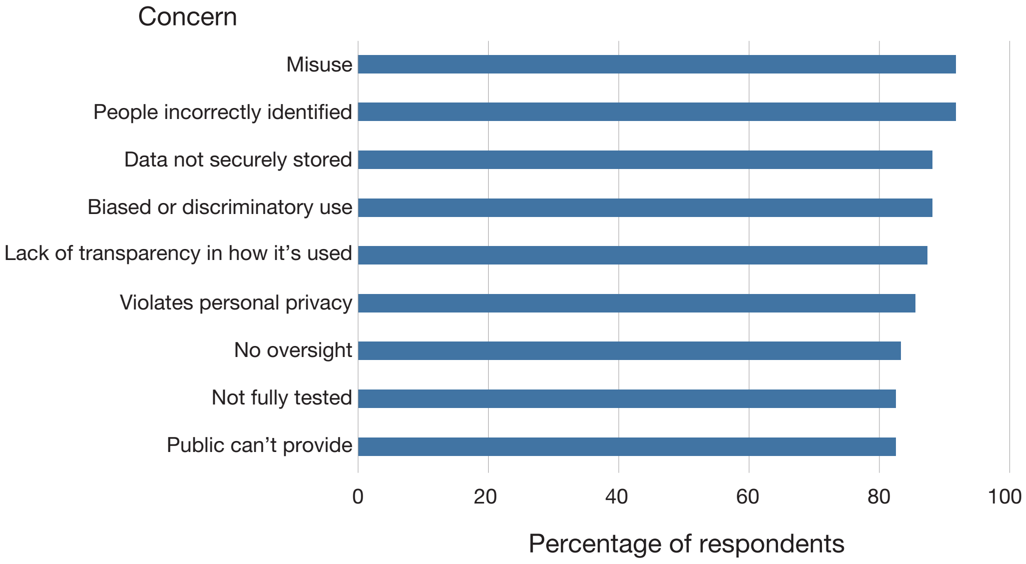
NOTE: The bars indicate the percentages of respondents who reported that this factor was very important or somewhat important in response to the question, “Which of the following are important for the U.S. government’s use of facial recognition technology?”

Respondents Reported Agreement That the Government's Use of Face Recognition Technology Raises Multiple Types of Risk, Including Misuse, Inaccuracy, and Bias

Respondents' answers about specific risks of government use of FRT suggest concerns about a broad variety of risks. More than 90 percent of respondents said that they thought misuse and inaccurate identification were significant risks. In fact, each of the nine potential risks were noted as such by at least 80 percent of respondents. These results, which could inform DHS risk-mitigation actions, indicate that the public would agree that many of the concerns that key stakeholders raised about government use of FRT are valid concerns. Figure 4.4 shows the broad variety of risks that the public would agree are concerns.

FIGURE 4.4

Perceived Risks of Government Uses of Face Recognition Technology



SOURCE: Features ALP data.

NOTE: The bars indicate the percentages of respondents who said that the item brought significant risk or some risk in response to the question, "Which of the following are risks of the U.S. government's use of facial recognition technology?"

Less Than One-Quarter of Respondents Reported Trusting the Government's Use of Face Recognition Technology

One research objective was to assess whether people's trust in DHS use of FRT differs from their trust in use by the broader U.S. government. Although survey results suggest that trust in both are low, the level of trust in the U.S. government's use of FRT is significantly lower than the level of trust in DHS's use of FRT, with 23 percent of respondents indicating agreement or strong agreement that they trusted U.S. government use of FRT, compared with 29 percent of respondents indicating agreement or strong agreement that they trusted DHS use of FRT. Certain factors were judged to be very important in the U.S. government's use of FRT; the majority of respondents judged accuracy (82 percent), security (81 percent), privacy (75 percent), fairness (69 percent), transparency (67 percent), oversight (61 percent), and ability to consent (55 percent) to be very important. On average, 9 percent of respondents answered, "don't know/it depends" (that response ranged between 5 percent and 14 percent for the nine questions about these factors).

Certain demographic groups were less likely to report agreeing that they trust both U.S. government and DHS use of FRT:[1]

- men less than women
- respondents identifying as liberal, conservative, and other partisan groups less than respondents who identified as "middle of the road"
- respondents ages 31 to 40 less than those ages 41 to 50 (the baseline group)
- those who reported using niche social media platforms either exclusively or in addition to mainstream social media less than people who had only a mainstream social media platform presence.

Conversely, those who identified as non-Hispanic Black or African American or non-Hispanic Asian or Pacific Islander were likelier to indicate agreement that they trusted both the U.S. government's and DHS's use of FRT than those who identified as non-Hispanic White or Caucasian.

Thirty-six percent of respondents provided either neutral or ambiguous responses about trusting U.S. government use of FRT, and 35 percent of respondents reported being either neutral or ambiguous about trusting DHS use of FRT.

Safeguards Could Improve the Public's Comfort with Government Use of Face Recognition Technology, but the Overall Effect Might Be Limited

Respondents were presented with a hypothetical scenario in which they were walking on the street by a government building, on which was posted a sign stating that the U.S. govern-

[1] Statistically significant differences ($p < 0.05$) were assessed using an ordinal logistic regression model.

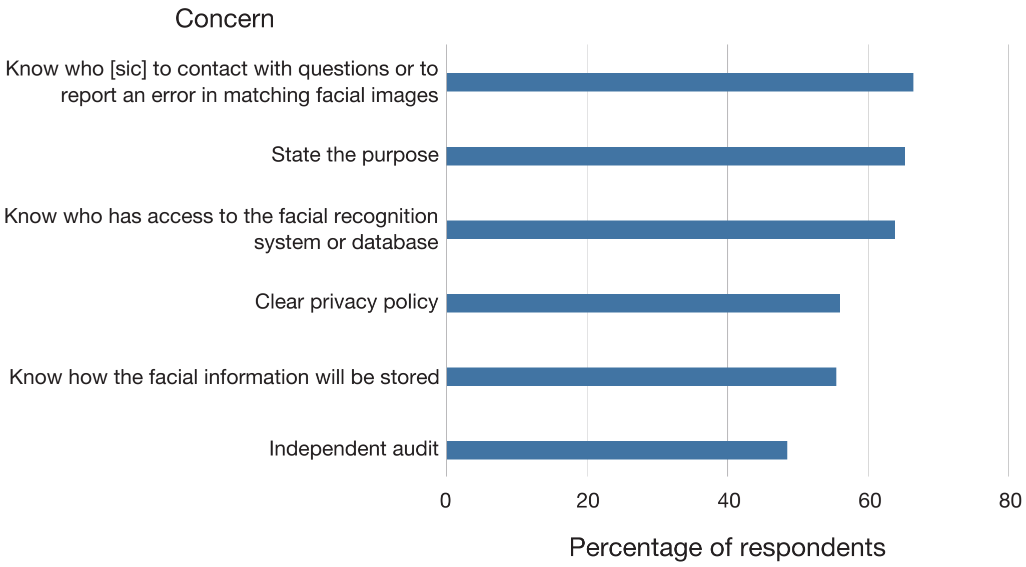
ment was using FRT on pedestrians. In this scenario, no additional information was provided about the intended use of the technology or whether one could opt out. Respondents were then asked about the degree to which different measures might improve their comfort level in this scenario. As shown in Figure 4.5, respondents expressed broad but limited support for these measures. All of the presented measures received similar levels of support, but none received support from more than approximately 60 percent of respondents. Thus, although a wide variety of measures might help the public feel more comfortable with government use of FRT, the impact of those measures is likely limited.

When asked to elaborate on what could make them more comfortable with this scenario, some respondents said that nothing would make them fully comfortable, while others expressed little concern, frequently saying they had nothing to hide. As one respondent it put it, "I do not have anything to hide, so, although I may not like it, I am comfortable with the facial recognition."

Other respondents described specific measures that would improve their comfort. For example, one respondent listed multiple safeguards that they thought were needed: "We need public debate and transparency over [sic] these policies before they are enacted; we need to document these debates and educate citizens, then give citizens a say before photographing people walking down the street." One respondent said simply, "Let me decide if I want to

FIGURE 4.5

Measures That Would Improve Comfort with Use of Face Recognition Technology Outside Government Buildings



SOURCE: Features ALP data.

NOTE: The bars represent the percentages of respondents who indicated that the measure would provide significant or some improvement in their comfort levels in response to the following question: "Which if any of the following would improve your comfort level in this scenario?"

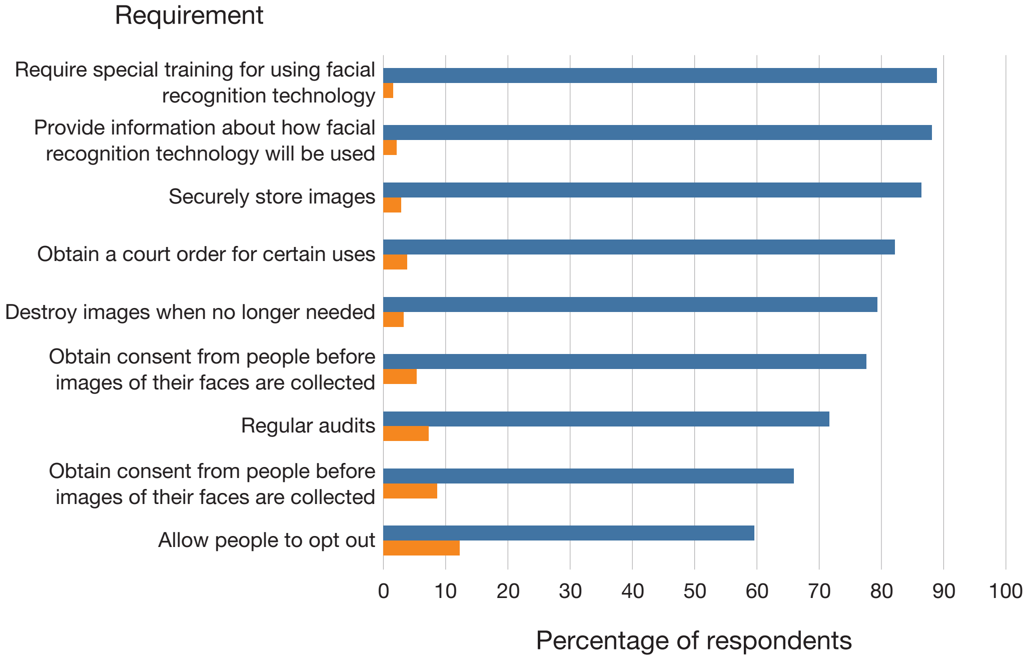
be involved or not." Yet another respondent directly acknowledged that even enacting the recommended safeguards might not eradicate their discomfort: "A statement saying that no photos taken of pedestrians are stored would help, but really I would be uncomfortable with this situation no matter what." This stance might make the public less willing to participate in some government technology deployments, as one respondent indicated: "I'm an honest citizen, with nothing to hide, but I will avoid walking around the premises."

Respondents Reported Believing That Government Should Have to Meet Certain Requirements for Using Face Recognition Technology

Respondents were asked their views on important requirements for the U.S. government's use of FRT. As shown in Figure 4.6, respondents said that they thought it most important that government users of FRT undergo special training and that the public should receive information about how FRT is being used. Other requirements to receive a substantial amount of support include getting a court order for use and meeting data storage requirements. Notably, about 10 percent of respondents said that they opposed two requirements that would allow

FIGURE 4.6

Important Requirements for Government Uses of Face Recognition Technology



SOURCE: Features ALP data.

NOTE: The blue bars represent the percentage who responded that the requirement was very important or somewhat important, and the orange bars indicate the percentage who said that it was not important in response to the following question: "Which of the following are important for the U.S. government's use of facial recognition technology?"

people to choose whether their data could be collected (9 percent for requiring consent and 12 percent for allowing people to opt out).

Respondents' Reported Support Depended More on the Application Than on the Technology

The survey included several parallel questions asking respondents whether they supported government use of different technology types (i.e., FRT, risk technology, LPR technology, and cell phone location data) for different government applications. These ten applications included identifying or tracking

- a suspect of a crime
- someone who appears likely to commit a crime
- someone suspected of violating immigration laws
- airport travelers
- students, teachers, or visitors at a school
- visitors to government buildings
- people in public spaces, such as parks or stadiums
- people in protests and demonstrations
- people at voting locations
- suspected terrorists at large public events.

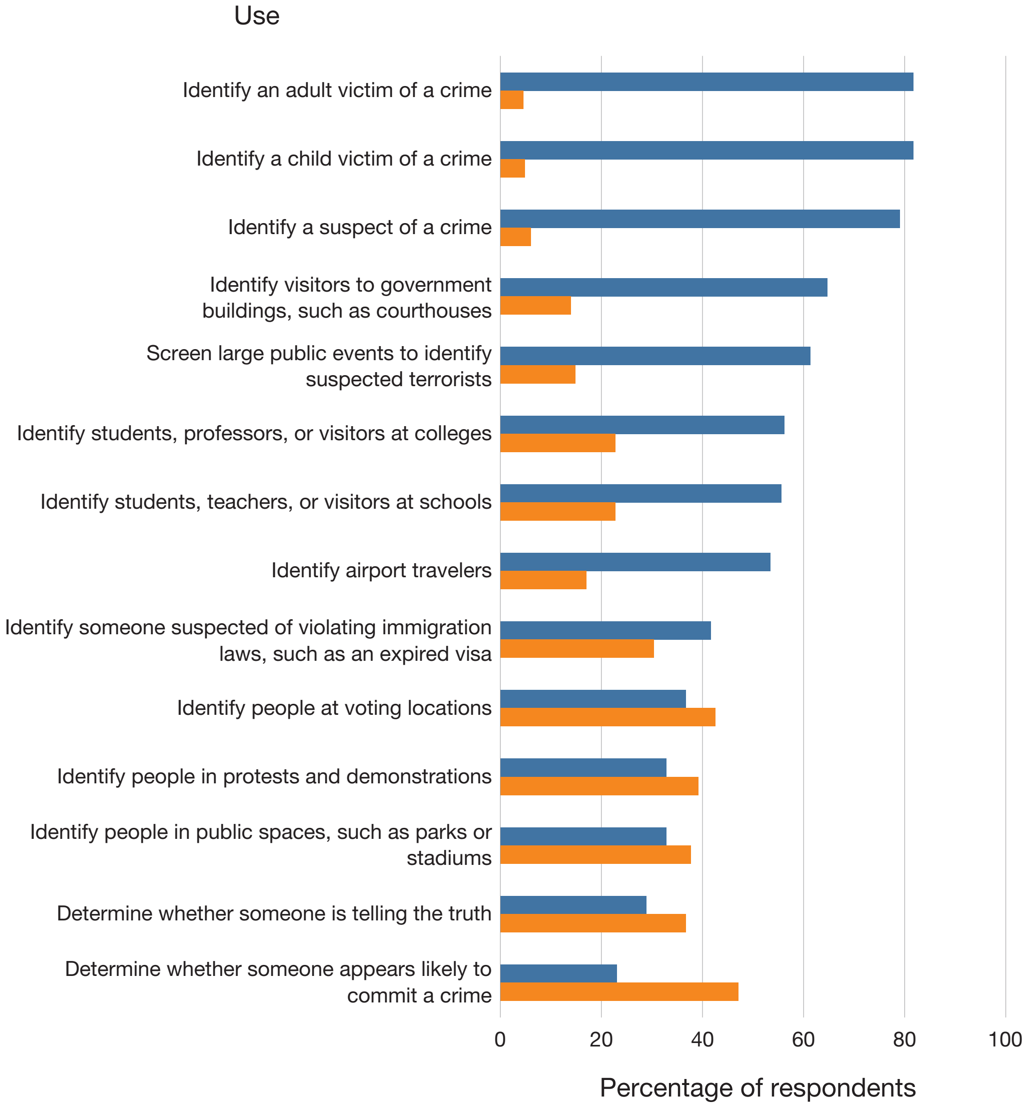
Responses were moderately to strongly correlated (*r* ranged from 0.55 to 0.78, all with $p < 0.001$) for both support and lack of support across different applications. This suggests that a respondent's reported support or lack of support for a given application did not change significantly based on the type of technology used—rather, what the specific application is might have had a stronger influence on whether respondents indicated their support. As discussed further in the next section, some specific applications of AI (such as for criminal investigations) received broad support regardless of the technology, whereas others received less support.

Respondents Reported Supporting Some Government Applications of Face Recognition Technology, Such as Criminal Investigations, but Not Others, Such as Identifying People at Protests or Public Spaces

Views on perceived benefits can be inferred from respondents' support for certain government applications of FRT. Figure 4.7 shows the percentage of respondents who said that they supported or strongly supported a given application, as well as the percentage of respondents who said that they opposed or strongly opposed it. The three most-supported government use cases were those using FRT to identify victims or suspects of crimes. However, responses were far less enthusiastic about the government using FRT to identify those suspected of vio-

FIGURE 4.7

Supported Government Uses of Face Recognition Technology



SOURCE: Features ALP data.

NOTE: The blue bars indicate the percentage of respondents who said that they supported or strongly supported this use, and orange bars indicate the percentage who said that they opposed or strongly opposed this use in response to the question, "The U.S. government might use facial recognition technology in many ways to safeguard the American people. How much do you support the following uses?"

lating immigration law, to identify people at public places or protests, or to determine whether someone seems likely to commit a future crime (this was the least-supported use). For each of those applications, more Americans would oppose the application than support it.

Several demographic characteristics are significantly associated with the level of support for multiple FRT applications (all p-values < 0.05). For each of the 14 FRT applications, we examined differential support by comparing demographic groups to a referent group:

- Compared with respondents with bachelor's degrees or some college experience, respondents with more than bachelor's degrees were less likely to indicate agreement with FRT use in all 14 applications.
- Compared with respondents who identified as "middle of the road" politically, respondents who identified as liberal were less likely to indicate agreement with FRT use in 11 of the 14 applications.
- Compared with women, men were less likely to indicate agreement with FRT use in eight of the 14 applications. For the other six applications, men and women did not differ.
- Additionally, compared with non-Hispanic White and Caucasian respondents, non-Hispanic Asian and Pacific Islander respondents were likelier to indicate agreement with FRT use in eight of the 14 applications, non-Hispanic Black and African American were likelier to indicate agreement with FRT use in five of the 14 applications, and Hispanic respondents were likelier to indicate agreement with FRT use in four of the 14 applications.
- Compared with respondents ages 41 to 50, respondents ages 61 to 75 were likelier to indicate agreement with FRT use in six of the 14 applications, and respondents over 75 years of age were likelier to indicate agreement with FRT use in seven of the 14 applications.
- Finally, compared with respondents with bachelor's degrees or some college experience, respondents with high school diplomas or less were likelier to indicate agreement with FRT use in six of the 14 applications.

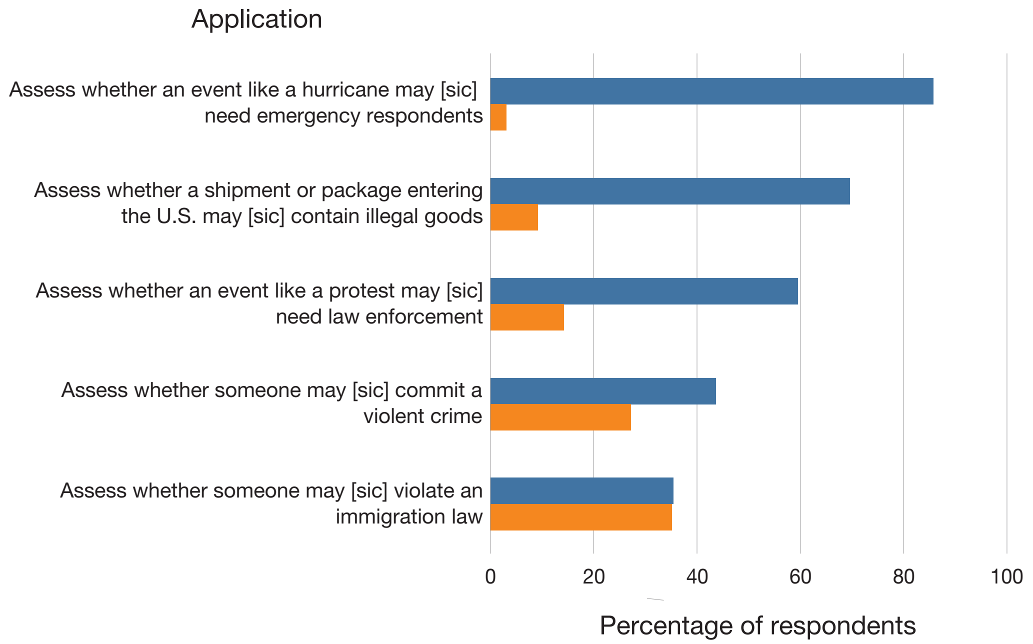
Public Perceptions of Risk Technologies

Risk technologies can use data to predict how likely it is that something will occur. Survey respondents were provided with examples of relevant use cases, such as whether a shipment contains illegal goods or whether a hurricane might create a need for emergency responders. They were then asked about their support for various uses of risk algorithms and data sources.

Respondents' Reported Support for Risk Technologies Varied by Application and Data Source

As shown in Figure 4.8, the use case with the most reported support is in the realm of disaster management, while less supported cases relate to law enforcement or immigration enforcement. The level of support reported across these use cases varies greatly, with 86 percent indicating support for the use of this technology to assess whether an incident needs emergency

FIGURE 4.8
Supported Government Applications of Risk Technology



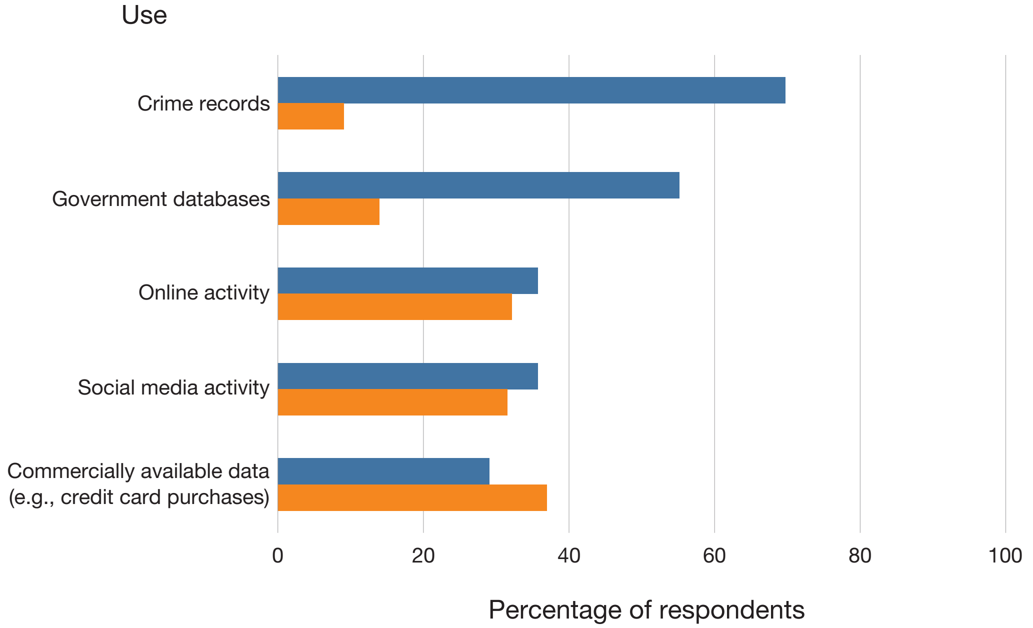
SOURCE: Features ALP data.

NOTE: The blue bars represent the percentage of respondents who said that they supported or strongly supported that application of risk technology, and orange bars represent the percentage of respondents who said that they opposed or strongly opposed that application of risk technology in response to the following question: “How much would you support or oppose the U.S. government’s use of risk technology for the following purposes?”

response, 44 percent indicating support for its use to assess whether someone might commit a crime, and only 36 percent indicating support for its use in assessing whether someone violated an immigration law.

Respondents were also asked whether they supported or opposed the U.S. government’s use of various data sources for risk technologies. As shown in Figure 4.9, the two government-owned data sources—crime records and government databases—are the only options for which more than half of respondents indicate support. The use of data based on online or social media activity or commercially owned data received support from no more than 40 percent of respondents.

FIGURE 4.9
Supported Government Uses of Data Sources for Risk Algorithms



SOURCE: Features ALP data.
NOTE: The blue bars represent the percentage of respondents who indicated that they supported or strongly supported these data sources, and orange bars represent the percentage who indicated that they opposed or strongly opposed these data sources in response to the following question: “How much would you support or oppose the U.S. government’s use of the following data sources to assess how likely it is that something may occur?”

Public Perceptions of License Plate Readers

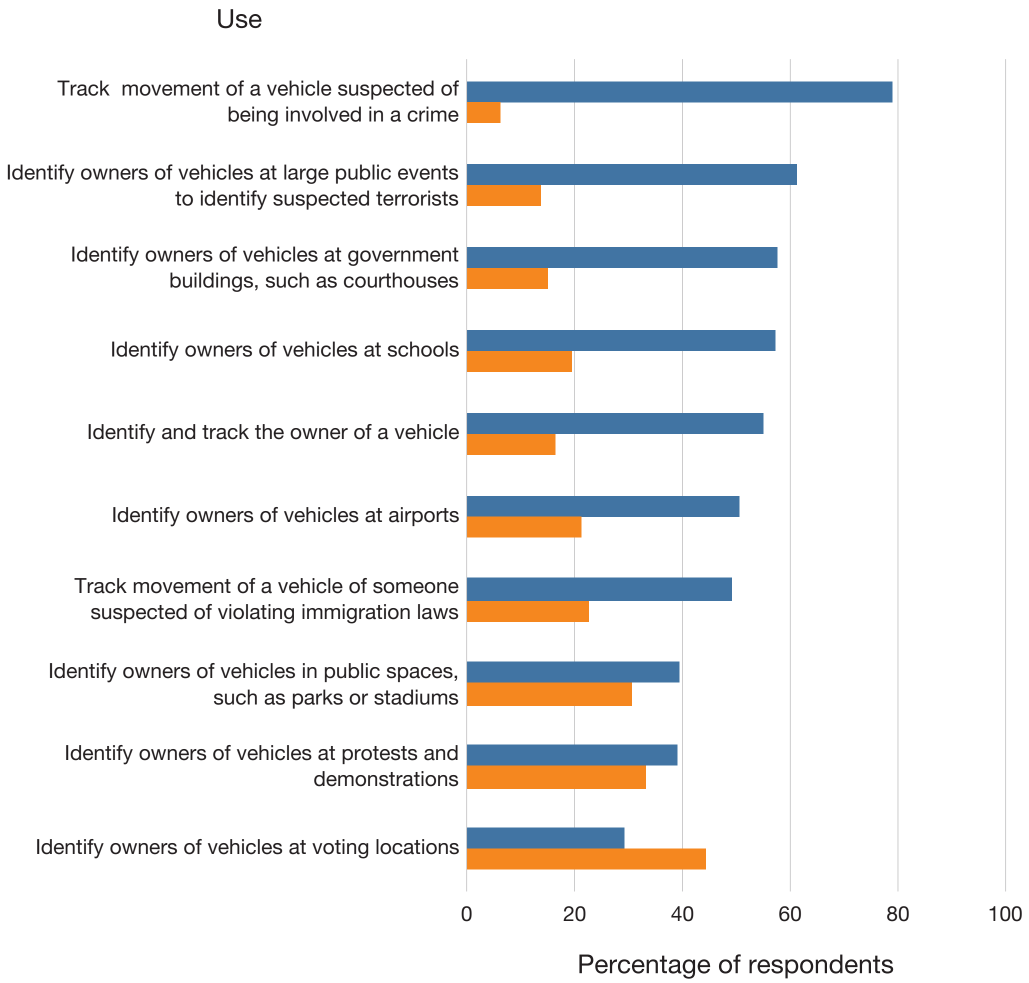
LPR technology uses computers to match license plates to records in a government database. Survey respondents were told that the U.S. government might use LPR technology in multiple ways and were asked their degree of support for various uses.

Respondents’ Reported Support for Government Use of License Plate Readers Varied by Application

As shown in Figure 4.10, respondents indicated being most supportive of LPRs to track movements of vehicles that might be involved in a crime and almost as supportive of uses that would identify suspected terrorists. Other uses received less support, with wide variance between the most and least supported uses. Using LPRs to identify owners of vehicles at voting locations, protests, or public spaces had the least support reported.

FIGURE 4.10

Supported Government Applications of License Plate Readers



SOURCE: Features ALP data.

NOTE: The blue bars represent the percentage of respondents who indicated that they supported or strongly supported the use of LPRs for that purpose, and orange bars represent the percentage who indicated that they opposed or strongly opposed that use for the following question: “The U.S. government might use license plate reader technology in multiple ways to safeguard its citizens. How much do you support the following uses?”

Respondents’ Reported Perceptions of Mobile Phone Location Data

Respondents were asked about the U.S. government’s use of mobile phone location data. Some private companies collect and sell location data collected from mobile phones, and the U.S.

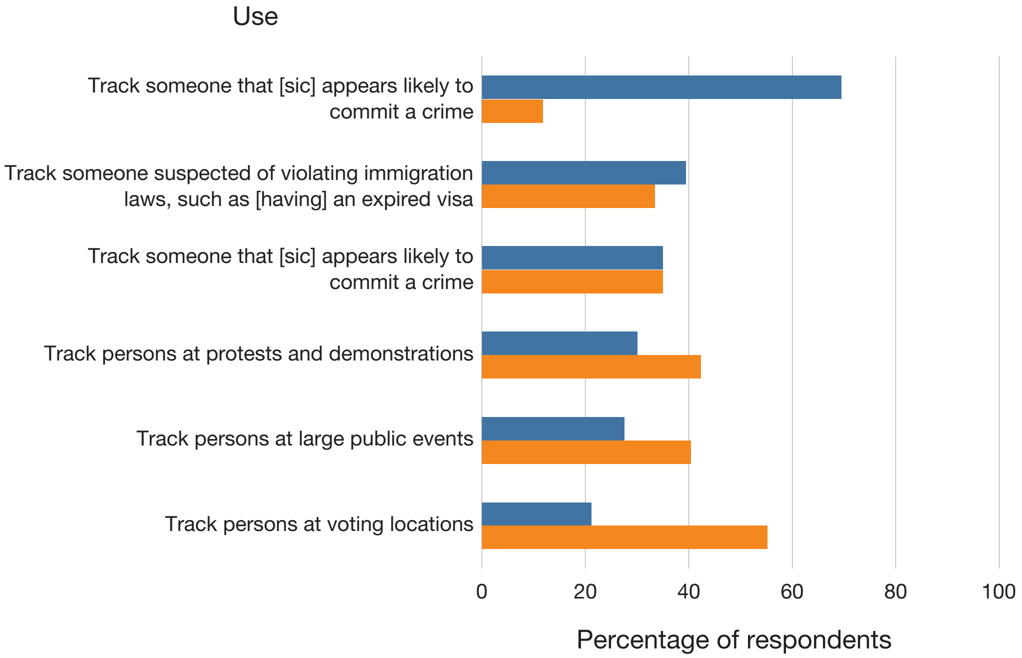
government (including DHS) has purchased such location data. These location data can be used to track people's movements or otherwise get information on places where people gather.

The Majority of Respondents Indicated Being Supportive of Using Location Data to Track Criminal Suspects but Not Being Supportive of Other Applications

As shown in Figure 4.11, respondents reported being by far most supportive of using mobile phone location data to track crime suspects. All other use cases received far less support—less than 50 percent.

FIGURE 4.11

Supported Government Applications of Mobile Phone Location Data



SOURCE: Features ALP data.

NOTE: The blue bars represent the percentage of respondents who indicated supporting or strongly supporting the use of mobile phone location data for that application, and orange bars represent the percentage who indicated opposing or strongly opposing in response to the following question: "The U.S. government might use cell [sic] phone location data in many ways to safeguard its citizens. How much do you support the following uses?"

CHAPTER 5

Recommendations and Conclusions

Public-perception research is important to help DHS build trust and support for its use of AI. We pursued one approach to evaluate public perception through the development and fielding of a nationally representative survey. The recommendations presented here suggest ways in which DHS can integrate public-perception studies, including the results from this public survey, into its acquisition, development, and fielding of AI technologies. Each of these recommendations is based on findings from our background research and the public survey.

Recommendations

Proactively Engage Communities That Are Uncertain or Neutral on Government Use of Artificial Intelligence

From our survey data, we can extrapolate that many members of the public are neutral, are unsure, or prefer not to express an opinion on the benefits and risks of FRT and other AI technologies. For some of the survey questions, these were the largest groups of respondents. DHS's ability to deploy AI will likely depend in part on reaching and gaining support from these communities.

Because AI technologies are developing rapidly, DHS might wish to consider proactively engaging communities with large proportions of members who express uncertainty or neutrality about particular uses of AI rather than waiting to respond to any observed reactions. This could involve research to identify in further detail the demographic and other characteristics of these communities and determine how best to engage them, such as through trusted community leaders, media, or targeted messaging.

As demonstrated by the fact that many respondents appeared to not yet have formed strong opinions of government use of technology, improving public understanding of these technologies could help clarify the relative benefits and risks. For example, if the public held ambiguous, inaccurate, or even negative views of a specific technology implementation, providing accurate information or other education could positively shift those views.

Deliberately Analyze Stakeholders' Perceptions of Benefits and Risks of Artificial Intelligence

Emerging technologies, such as AI, might provide crucial support to key homeland security missions, presenting such benefits as enhanced security and convenience for Americans in a variety of contexts. However, those same technologies carry risks, as evidenced by concerns raised by influential stakeholders. The survey results suggest that members of the American public perceive some benefits to DHS uses of AI while also harboring concerns about risks of those uses. In fact, we can infer that only about 40 percent of Americans believe that the benefits of DHS use of FRT outweigh the risks and that Americans perceive a broad set of risks in government use of FRT and other AI. As mentioned already, we can extrapolate that a large proportion of other Americans are neutral or uncertain of their views of government use of AI. In addition, we can infer that Americans agree that certain issues, such as security and privacy, are more important than speed or convenience for the government's use of FRT.

Accordingly, DHS could take steps to better gauge and understand the public's views about benefits and risks, particularly how those views differ among various groups. Such knowledge could inform more-detailed steps to mitigate the concerns, such as the steps discussed toward the end of this list of recommendations. The survey results reported here offer a first look at these perceptions, but a more nuanced picture of public opinion is needed. Our initial results should be further tested through additional analyses of existing data (e.g., cluster analysis) or additional data collection, such as experimental designs that could identify more-specific correlations based on technology type.

Other recommendations in this section provide additional detail on how DHS might mitigate public concern, but an important approach is to deliberately seek to uncover perceptions of specific benefits and risks.

An additional approach would involve messaging. DHS could consider implementing communication strategies around its uses of AI that address both the benefits and the risks, rather than focusing strictly on one or the other. This could involve a broad, comprehensive strategy that attempts to address multiple aspects at once; leveraging certain perceptions of benefit; or targeting specific groups' concerns. For example, investigating crimes was one use of AI that garnered broad support. DHS could consider focusing on AI applications in this domain or publicizing its successes. This might improve trust that DHS is using AI in applications the public supports.

When Choosing How to Implement an Artificial Intelligence Technology, Focus on Applications and Safeguards Rather Than on the Type of Technology

The results of our survey indicate that public support is less related to which technology is used (e.g., FRT versus LPRs) than it is to the purpose or role of the DHS application. This suggests that key aspects of communication around AI implementations should go beyond the specifics of the technology and should include the purposes, processes, and safeguards to ensure that the narrow uses are clearly explained.

DHS should carefully consider the results of the public survey to ensure that the department is focusing on AI applications that receive broad support (such as identifying victims of crimes), and it should be especially cautious in deployments of AI applications for uses that are less well-supported (such as predicting who will commit a crime or using AI technologies at protests or in public spaces). Using AI for these nonsupported applications might raise public ire in ways that could affect DHS's ability to use these technologies in supported applications. However, if DHS proactively asserts that it will focus on narrow applications that the public is likely to support, this might encourage technology companies to partner with DHS or Congress to support DHS use of AI. Through careful use in narrow applications, DHS could demonstrate responsible use of AI in a way that might build public support for additional use cases.

Insofar as it pursues less supported applications, DHS should build stringent and broad safeguards that the research findings suggest might help increase public support for AI uses, including providing proper notice and consent and being subject to external review and oversight.

Consider Which Data Sources Underpin Artificial Intelligence

Survey respondents reported support for the use of government-owned data sources, such as criminal records, more than for other sources of data that underpin AI tools, such as social media data. This finding might suggest an opportunity for DHS to exploit the data it already holds or to which it has access rather than looking to commercially available or open-source data. In-house data have practical advantages, such as accessibility and cost. Moreover, it is likely that regulators already have the clear authority and procedural ability to use the data. However, if commercially available AI tools rely on external data, they might raise questions about data provenance and handling, be unusable, or require retraining on government-owned data.

Companies that collect data through social media or internet scraping have come under scrutiny for their data-harvesting practices, drawing attention from Congress and advocacy groups. These survey results suggest that the public would be concerned about DHS's reliance on companies that collect data through these practices. Although commercial data offer a breadth of information beyond what DHS currently can access, the benefits of relying on these data might be short-lived if the public does not support their use, leading to longer-term reputational costs and perhaps even legal jeopardy.

Build Trust in the Department of Homeland Security and the Rest of the U.S. Government Through Continued Partnerships

Respondents indicated low levels of trust in both DHS and the broader U.S. government regarding the use of AI technologies. For example, when asked about their comfort with a hypothetical government use of face recognition, one respondent said,

> I have so little trust in our government at the moment; it's hard to imagine them using this technology without perpetuating corruption and abuse. In theory, there are many benefits to such a system . . . It's a bit like a pandora's box of worms [sic] . . . but I just don't trust our law enforcement or government agencies to be responsible.

Because the findings from this survey match what other surveys have revealed, they are not surprising, but they underscore how crucial it will be for the government to build trust with the public. As another respondent put it, "I have a certain baseline distrust with the government's use of facial recognition technologies, but it might just be caused by a distrust of the government at large, but that's their fault." This is a large and complex problem—DHS can seek to make progress in many areas, while we have addressed only a specific instance in which public-perception studies can help. For instance, Kavanagh and her colleagues (2020) laid out a set of attributes that institutions must demonstrate (such as competence, accuracy, and transparency) to win public trust, and public-perception studies can help identify specific demographic characteristics of those who agree or disagree that institutions meet those attributes. Further, we have discussed how identifying "neutral" respondents provides DHS an opportunity to proactively educate and engage. In addition, findings from our survey suggest a path for DHS to follow by focusing on the use of AI technologies in narrow applications to ensure that the department is building a variety of safeguards to use, such as those safeguards the public supports. DHS should also prioritize such issues as accuracy, privacy, and security over convenience or speed to help build trust in those use cases.

Our findings indicate that DHS should identify ways that continue and expand its work with partners at the community level; advocacy groups; state, local, tribal, and territorial entities; and technology companies, among others, to understand public views and seek to build overarching trust. Such trust-building efforts could include regular engagement, such as standing meetings with key public stakeholders to discuss areas of shared interest or concern, or messaging to the broader public. It might also be helpful in these engagements to emphasize trust-building as an explicit goal and to request assistance from stakeholder groups that can connect DHS with communities with limited trust.

Consider Partisanship's Impact on Views of Artificial Intelligence

Many survey respondents did not want to state their political views, and the number of public comments (during the survey vetting process) and questions from survey respondents suggests that partisanship in government use of technology is a particularly sensitive topic. This finding echoes the broader debate about the proper role of technology in society, in which opinions are often divided along ideological lines. For instance, tech companies are sometimes accused of harboring political biases, such as in their workforces or decisionmaking.

Given this context, DHS should consider whether current or planned AI implementations could engender similar partisan debate or become enmeshed in existing debates. DHS could consider, for example, ways to demonstrate that it has implemented sufficient processes to ensure that these powerful technologies will not be used in ways that either appear partisan or in fact unequally affect people of certain ideologies. This effort could also involve exploring how to avoid triggering partisan reactions, such as research about the types of partisan concerns that have hindered adoption of other technology uses in the past.

It might also be important to better understand why survey respondents who did not wish to state their political leanings were also likelier to decline to respond to the questions about use of AI. The unknown reasons behind this connection constitute a specific knowledge gap about a population group that wishes neither their political leanings nor their views on technology to be known.

Use Multiple Methods to Routinely Engage Key Stakeholders

Stakeholders can affect DHS technology deployments in different ways. For example, members of the public can choose whether to opt out of using a technology (e.g., face recognition at airports); technology companies can choose whether to sell to the U.S. government; members of Congress might control whether funding continues. For each of these constituencies, taking different approaches to evaluating public perception might provide diverse insight and perspectives. For example, focus groups held before announcement of the Disinformation Governance Board might have revealed concerns that would predict possible backlash against the board.

Conducting routine engagement through multiple data collection methods could emphasize seeking a diversity of perspectives. Actively using multiple methods helps tap different stakeholder groups, but, at minimum, routine engagement could include passively collecting the perspectives of diverse stakeholders by using observational techniques or secondary data. Table 5.1 describes several such methods and a subset of their respective benefits and drawbacks.

Integrate Public Perceptions into Technology Development and Acquisition Life Cycles

Societal concerns about how technology is widely deployed, such as privacy or public perceptions, should be considered in all phases of technology deployment. Often, according to our DHS interviews, such considerations are limited to impact assessments, either while technology deployments are still being considered or after the bulk of technology deployment and implementation are completed. In the former case, the technology and its use cases might be too unclear to shape meaningful mitigations to potential concerns; in the latter, the technology deployments are too far along to shift or reverse course.

TABLE 5.1
Examples of Methods to Engage Public Stakeholders

Method	Description	Benefit	Drawback
Elicited[a]			
Interview	Questions posed to an individual	• In-depth exploration of individual perceptions	• Can be resource intensive • Depending on design, can be difficult to generalize
Focus group	Questions posed to a small group (around six to 12 people)	• Balances depth and breadth of perceptions in a social, interactive setting	• Answers capable of being influenced by other group members • Difficult to communicate or implement findings
Survey	Series of questions on topics of interest distributed to a sample of people	• Efficient • Structured, replicable, generalizable (with appropriate sampling) • Easier to communicate or implement findings than with focus groups	• Difficult to get sufficient response rate • Can be hard to capture nuanced dimensions of perceptions in depth • Not necessarily a reliable predictor of behavior
Observed			
Content analysis	Process of identifying certain words, concepts, or themes present in some form of text data (e.g., a transcript)	• Systematic • Low unit costs	• Potentially high up-front costs
Behavioral observation	Collection of data on behavior in a natural environment (e.g., search history or market analysis)	• Can help support external validity of research • Can provide valid and reliable measures that do not rely on self-reported data	• Difficult to control outside variables • Behaviors possibly influenced by others in the social setting

SOURCE: Adapted from Boudreaux, Yeung, and Steratore, 2022, p. 13.

[a] Elicited methods might be subject to the requirements of the PRA, a federal law mandating certain authorizations from OMB in order for a federal agency to collect information on members of the public for certain applications. These methods will also be subject to human-subject protection requirements.

Information about public perceptions and other societal considerations could be integrated into various elements of technology development and acquisitions. Table 5.2 describes examples of ways in which this could be done. That information could then be used to build safeguards for how technology is used, inform messaging that might explain benefits or risks of using the technology, or shape the technology applications themselves.

TABLE 5.2

Select Ways to Integrate Public Perceptions into Technology Acquisition and Deployment

Element of Technology Acquisition and Deployment	Select Ways to Integrate Public Perception, Using Multiple Techniques
Acquisition planning	• Identify the public's views about benefits and concerns about the proposed technologies in non-DHS use cases. • Explore the public's views about the specific DHS purpose for which the technology is proposed. • To understand their concerns, engage members of communities likely to be most affected by the technology use case. • Use public-perception information as a key consideration within cost–benefit analysis associated with technology planning.
Solicitation and selection	• Explore the public's views about specific technology companies' data privacy and other practices (e.g., scraping online social media photos). • Identify views expressed by key technology developers about government use of the technology (e.g., Microsoft and Amazon as developers of FRT used by governments). • Use public-perception information as a key consideration within technology solicitation processes to tailor solicitations and develop solicitation criteria that best align with public attitudes and address concerns.
Development	• Consider the public's views on the technical limitations associated with the technology. • Consider operational partners' views about technology development approaches and standards. • Use public-perception information as a key consideration to build relevant policy, procedural, and technical criteria into the development process.
Delivery	• Develop strategic communications that leverage risk-communication best practices. • Tailor messages to different communities to correct misinformation and to assuage concerns. • Consider the views of DHS end users and ensure that users understand and support the use of the technology.
Deployment and maintenance	• Deploy technology in ways consistent with information about public perception (e.g., location, proper purpose, allowing people to opt out). • Consult regularly with the communities affected by the technology. • Continue to refine and deliver strategic communications. • Consider potential effects on any agency that deploys the technology (e.g., workforce morale, integration into existing processes.

SOURCE: Adapted from Boudreaux, Yeung, and Steratore, 2022, p. 19.

Ensure That Insights About Public Perceptions of Technology Are Timely

Public perceptions of government technology use can shift rapidly based on world events or policy changes. By routinely monitoring public perceptions of technology, DHS could ensure that it has current insight that might influence technology deployments. This would include insight into important trends, such as how public views might change over time, or as different types of technology emerge and come under consideration for DHS deployment.

Routine monitoring of public perceptions could also lead to other important benefits, such as demonstrating to the public that DHS considered public views to be important and was taking steps to incorporate those views into decisionmaking and implementation. Routinizing collection of data on perceptions could also help integrate such collection into technology acquisitions, the way privacy reviews and vendor selection are. Finally, timely insight could help inform engagement with key stakeholders.

To increase timeliness, the government might seek lessons from technology companies that continually research reactions to technology before they are deployed, including through A/B testing and other ways to assess how people will actually engage with the technology. This could help demonstrate the benefits that can accrue from certain technology programs or how to implement consent and opt-out mechanisms that empower the public. It is, of course, likely that the government has to follow certain regulations that the private sector does not, and that could limit its abilities relative to research techniques that tech companies use, but it might be helpful to explore what is possible.

Besides making public-perception research a routine practice, DHS could also explore ways of minimizing existing constraints on it. Because public-perception research generally entails asking people about their attitudes about various topics, it is subject to regulations and procedures that could limit efficiency. For example, one such constraint involves obtaining necessary approvals that ensure ethical research. Many active data collection methods (i.e., surveys, interviews) are rightly considered human-subject research and thus are subject to stringent review to ensure that the research is conducted ethically (whereas other, passive techniques, such as analyzing publicly observable data, such as social media, might require less review). Such processes can be lengthy. Institutional review board approvals for human-subject research can take weeks or months. Subsequently obtaining multiple government approvals, such as those from DHS privacy offices and satisfying PRA requirements, can take months or even years. DHS could try to shorten such processes in several ways, such as by developing templates for public-perception research with standardized information so that new projects could more quickly apply for approval or by binning multiple research topics that would require a single project approval.

Conclusion

We fielded a nationally representative survey, using ALP, to gather public perceptions of government use of AI, such as face recognition. We synthesized the results to identify trust in and support for DHS applications of AI. These results informed recommendations that DHS can use to guide the acquisition, development, and deployment of these technologies. Going forward, developing an approach to routinely assessing public perceptions of AI and other emerging technologies could benefit DHS's ability to implement those technologies in support of its homeland security mission while maintaining legitimacy and support of the American public.

APPENDIX A

Public Perception of Artificial Intelligence Survey Instrument

This appendix provides the survey instrument, unaltered except formatting response matrices to fit the page, that was used in ALP to collect the data used for this study.

Public Perception of Emerging Technology: Survey Instrument

Thank you for taking the time to participate in our survey. First, we'd like to tell you a bit about the project, how your responses will be used, and your rights as a research participant.

We are researchers with the Homeland Security Operational Analysis Center, one of the Department of Homeland Security's (DHS) Federally Funded Research and Development Centers, operated by the RAND Corporation, which is a nonprofit policy research organization. We are conducting research to support the DHS Science and Technology Directorate regarding public perceptions of the use of emerging technology.

The purpose of this survey is to understand your views on the U.S. government's use of new technologies. You will be asked a variety of questions, and your responses will be used by DHS to understand public views on this topic. There are no right or wrong answers, and we value everyone's perspective.

No one outside of the project team will have access to your responses. RAND has strict information protection protocols in place to prevent any disclosure of your participation in this survey. However, inadvertent disclosure of your responses might pose minimal risk to your financial standing, employability, educational advancement, or reputation.

The research team will not have access to personally identifiable information about you. Reports of the survey findings will be provided at a summary level to

DHS that would not reveal or allow your identity to be inferred. Raw data from survey responses will not be shared with DHS.

The survey will take about 16 minutes of your time. Your participation in this survey is strictly voluntary. You are free to skip any question you do not wish to answer. You can stop participation at any time and opt out of future research.

Please direct any questions you have about this study to the project leaders listed below and any questions about your rights as a research participant to RAND's Human Subjects Protection Committee.

Whom to Contact About This Research:

Project Leaders: Benjamin Boudreaux, bboudrea@rand.org, 310-393-0411x6917 and Douglas Yeung dyeung@rand.org, 310-393-0411x7939.

If you have questions about your rights as a research participant or need to report a research-related concern, you can contact RAND's Human Subjects Protection Committee toll-free at (866) 697-5620 or by emailing hspcinfo@rand.org.

Introduction

The purpose of this survey is to explore your views on the U.S. government's use of new technologies. You will be asked about:

- **Part 1: Facial Recognition Technology** that uses computers to match faces from a photo or video to faces from a database.

- **Part 2: Risk Technology** that assesses how likely it is that something will occur.

- **Part 3**: **License Plate Reader Technology** that uses computers to identify or match license plates (or car tags) from a state-run database.

- **Part 4: Cell Phone Location Tracking** that uses cell phone location data to track movement.

Part 1: Facial Recognition Technology

The following questions ask about your knowledge and use of facial recognition technology.

Facial recognition technology uses computers to match faces from a photo or video to faces from a database.

1. **What comes to mind when you hear "facial recognition technology?" Please do not include any personal information (such as your name, address, email or phone number).**

____

2. **Do you use facial recognition technology, for instance, to unlock your phone?**

   □ Yes
   □ No
   □ Don't Know
   □ Prefer not to say

3. **Are you aware of a time when facial recognition technology was used to identify or learn about you?**

   □ Yes, I am aware
   □ No, I am not aware
   □ Prefer not to say

4. **How much do you agree or disagree with the following?**

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Don’t Know/ It Depends	Prefer not to Say
There are benefits of facial recognition technology	□	□	□	□	□	□	□
There are risks of facial recognition technology	□	□	□	□	□	□	□
Overall, the benefits of facial recognition technology outweigh its risks	□	□	□	□	□	□	□

The following questions ask about the U.S. government’s use of facial recognition technology.

5. **Are you aware of examples of the U.S. government’s use of facial recognition technology?**

□ Yes, I am aware
□ No, I am not aware
□ Prefer not to say

6. How much do you agree or disagree with the following?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Don’t Know/ It Depends	Prefer not to Say
There are benefits of the U.S. government’s use of facial recognition technology	☐	☐	☐	☐	☐	☐	☐
There are risks of the U.S. government’s use of facial recognition technology	☐	☐	☐	☐	☐	☐	☐
Overall, the benefits of U.S. government use of facial recognition technology outweigh its risks	☐	☐	☐	☐	☐	☐	☐
I trust the U.S. government’s use of facial recognition technology	☐	☐	☐	☐	☐	☐	☐
I trust the Department of Homeland Security’s use of facial recognition technology	☐	☐	☐	☐	☐	☐	☐

7. **Which of the following are important for the U.S. government's use of facial recognition technology?**

	Very Important	Somewhat Important	Not Important	Don't Know/It Depends	Prefer not to Say
Ability to consent	□	□	□	□	□
Accuracy	□	□	□	□	□
Convenience	□	□	□	□	□
Fairness	□	□	□	□	□
Oversight	□	□	□	□	□
Privacy	□	□	□	□	□
Security	□	□	□	□	□
Speed	□	□	□	□	□
Transparency	□	□	□	□	□

8. **Which of the following are risks of the U.S. government's use of facial recognition technology?**

	Significant Risk	Some Risk	No Risk	Don't Know/It Depends	Prefer not to Say
Public can't provide consent	□	□	□	□	□
People incorrectly identified	□	□	□	□	□
Misuse	□	□	□	□	□
Biased or discriminatory use	□	□	□	□	□
No oversight	□	□	□	□	□
Violates personal privacy	□	□	□	□	□
Data not securely stored	□	□	□	□	□
Not fully tested	□	□	□	□	□
Lack of transparency in how it's used	□	□	□	□	□

9. The U.S. government might use facial recognition technology in many ways to safeguard the American people. How much do you support the following uses?

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Identify a child victim of a crime	□	□	□	□	□	□	□
Identify an adult victim of a crime	□	□	□	□	□	□	□
Identify a suspect of a crime	□	□	□	□	□	□	□
Determine whether someone appears likely to commit a crime	□	□	□	□	□	□	□
Identify someone suspected of violating immigration laws such as an expired visa	□	□	□	□	□	□	□
Identify airport travelers	□	□	□	□	□	□	□
Identify students, teachers, or visitors at schools	□	□	□	□	□	□	□
Identify students, professors, or visitors at colleges	□	□	□	□	□	□	□
Identify visitors to government buildings such as courthouses	□	□	□	□	□	□	□
Identify people in public spaces such as parks or stadiums	□	□	□	□	□	□	□

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Identify people in protests and demonstrations	□	□	□	□	□	□	□
Identify people at voting locations	□	□	□	□	□	□	□
Screen large public events to identify suspected terrorists	□	□	□	□	□	□	□
Determine whether someone is telling the truth	□	□	□	□	□	□	□

10. How much would you support or oppose the following requirements for the U.S. government's use of facial recognition technology?

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Allow people to opt out	□	□	□	□	□	□	□
Regular audits	□	□	□	□	□	□	□
Destroy images when they are no longer needed	□	□	□	□	□	□	□
Obtain a court order for certain uses	□	□	□	□	□	□	□
Obtain consent from people before images of their face are collected	□	□	□	□	□	□	□

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Obtain consent from people if images of their face will be shared	□	□	□	□	□	□	□
Provide information about how the facial recognition technology will be used	□	□	□	□	□	□	□
Require special training for using facial recognition technology	□	□	□	□	□	□	□
Securely store images	□	□	□	□	□	□	□

11. How much would you support or oppose the U.S. government's use of photos from these sources for facial recognition technology?

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Driver's license photos	□	□	□	□	□	□	□
Photos of arrestees	□	□	□	□	□	□	□
Photos of convicted criminals	□	□	□	□	□	□	□
Passport or visa photos	□	□	□	□	□	□	□
Photos openly available on the Internet	□	□	□	□	□	□	□
Photos shared by users of social media sites	□	□	□	□	□	□	□

The next set of questions ask about a hypothetical use of facial recognition technology.

12. You are walking down the street and pass by a government building. You notice a sign on the building. It states that U.S. government officials are using facial recognition technology on pedestrians. It is not clear why or if you can opt out.

a. What is your comfort level with this scenario?

□ Very Comfortable
□ Comfortable
□ Uncomfortable
□ Very Uncomfortable
□ Don't Know
□ Prefer not to say

b. Which if any of the following would improve your comfort level in this scenario?

	No Improvement in comfort level	Some Improvement in comfort level	Significant Improvement in comfort level	Don't Know/It Depends	Prefer not to Say
Clear privacy policy	☐	☐	☐	☐	☐
State the purpose	☐	☐	☐	☐	☐
Independent audit	☐	☐	☐	☐	☐
Know how the facial information will be stored	☐	☐	☐	☐	☐
Know who has access to the facial recognition system or database	☐	☐	☐	☐	☐
Know who to contact with questions or to report an error in matching facial images	☐	☐	☐	☐	☐

c. Would anything else improve your comfort level with this scenario? Please describe. **Please do not include any personal information (such as your name, address, email or phone number).**

____

Part 2: Risk Technology to Assess how Likely Something Will Occur

The following questions ask about the U.S. government's use of risk technology to assess how likely it is that something will occur.

Risk technology can use data to assess how likely it is that something may occur. Examples include whether a shipment contains illegal goods or if a hurricane may need emergency responders.

13. **Are you aware of times when computers have used data to learn about you?**

    □ Yes, I am aware

    □ No, I am not aware

    □ Prefer not to say

14. **How much would you support or oppose the U.S. government's use of risk technology for the following purposes?**

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Assess whether someone may commit a violent crime	□	□	□	□	□	□	□
Assess whether someone may violate an immigration law	□	□	□	□	□	□	□
Assess whether a shipment or package entering the U.S. may contain illegal goods	□	□	□	□	□	□	□
Assess whether an event like a hurricane may need emergency responders	□	□	□	□	□	□	□
Assess whether an event like a protest may need law enforcement	□	□	□	□	□	□	□

15. **How much would you support or oppose the U.S. government's use of the following data sources to assess how likely it is that something may occur?**

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Commercially-available data (e.g., credit card purchases)	□	□	□	□	□	□	□
Crime records	□	□	□	□	□	□	□
Government databases	□	□	□	□	□	□	□
Online activity	□	□	□	□	□	□	□
Social media activity	□	□	□	□	□	□	□

Part 3: License Plate Reader Technology

The following questions ask about the U.S. government's use of license plate reader technology.

License plate reader technology uses computers to identify or match license plates (or car tags) from a government database.

16. **Are you aware of times when license plate reader technology was used on your vehicle?**

□ Yes, I am aware
□ No, I am not aware
□ Prefer not to say

17. **The U.S. government might use license plate reader technology in multiple ways to safeguard its citizens. How much do you support the following uses?**

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Identify and track the owner of a vehicle	□	□	□	□	□	□	□

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Track movement of a vehicle suspected of being involved in a crime	□	□	□	□	□	□	□
Track movement of a vehicle of someone suspected of violating immigration laws	□	□	□	□	□	□	□
Identify owners of vehicles at airports	□	□	□	□	□	□	□
Identify owners of vehicles at schools	□	□	□	□	□	□	□
Identify owners of vehicles at government buildings such as courthouses	□	□	□	□	□	□	□
Identify owners of vehicles in public spaces such as parks or stadiums	□	□	□	□	□	□	□
Identify owners of vehicles at protests and demonstrations	□	□	□	□	□	□	□
Identify owners of vehicles at voting locations	□	□	□	□	□	□	□
Identify owners of vehicles at large public events to identify suspected terrorists	□	□	□	□	□	□	□

Part 4: Cell Phone Location Tracking

The following questions ask about the U.S. government's use of cell phone location data. Some private companies collect and sell location data from cell phones. The U.S. government has purchased such location data in the past. These location data can be used with computers to track people's movements.

18. The U.S. government might use cell phone location data in many ways to safeguard its citizens. How much do you support the following uses?

	Strongly Support	Support	Neither Support nor Opposed	Opposed	Strongly Opposed	Don't Know/ It Depends	Prefer not to Say
Track someone suspected of committing a crime	□	□	□	□	□	□	□
Track someone that appears likely to commit a crime	□	□	□	□	□	□	□
Track someone suspected of violating immigration laws such as an expired visa	□	□	□	□	□	□	□
Track persons at protests and demonstrations	□	□	□	□	□	□	□
Track persons at voting locations	□	□	□	□	□	□	□
Track persons at large public events	□	□	□	□	□	□	□

Questions About You

The next question asks about media sources you use.

19. Please select up to two sources you rely on the most for news.

Sources you use the most for news	
	Select up to 2
Blogs	□
Friends and family	□
Professional colleagues	□
Email newsletters	□
Podcasts	□
Print news magazines	□
Print newspapers	□
Radio	□
Social media sites	□
Television	□
News websites	□

The next two questions ask about your use of technologies, products, and services.

20. Please rate how much you agree or disagree with the following:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	Don't Know/ It Depends	Prefer not to Say
I am generally aware of new technologies, products, or services.	□	□	□	□	□	□	□
I feel comfortable using new technologies, products, and services.	□	□	□	□	□	□	□
I try new technologies, products, or services before other people do.	□	□	□	□	□	□	□
When I try new technologies, it is because I like variety and get bored with the same old thing.	□	□	□	□	□	□	□

21. How many total hours per week do you typically use technologies? This can include your computer, smart phone, tablet, smart watch, or video games?

□ Less than 1
□ 1-10
□ 11-20
□ 21-30
□ 31-40
□ 41-50
□ 50+
□ Don't Know
□ Prefer not to say

The next set of questions ask about your use of social media.

22. Which if any social media sites do you use? Please check all that apply.

□ Facebook
□ Instagram
□ LinkedIn
□ Parler
□ Pinterest
□ Reddit
□ Snapchat
□ TikTok
□ Twitter
□ WhatsApp
□ YouTube
□ Other
□ None
□ Don’t Know
□ Prefer not to say

23. How often do you share photos or videos on social media sites?

□ Multiple times a day
□ Daily
□ Weekly
□ Monthly
□ Never
□ Don’t know
□ Prefer not to say

The next question asks about your background in computer science, programming, or Information Technology.

24. Do you have an educational or professional background in computer science, programming, or Information Technology (IT)?

□ Yes
□ No
□ Prefer not to say

The next question asks about the level of trust you have in various institutions in society.

25. How much do you trust each of the following institutions to act in a way that you agree with?

	A Great Deal	Quite a Lot	Some	Very Little	None
Digital media such as social media, blogs, or podcasts	□	□	□	□	□
The Department of Homeland Security	□	□	□	□	□
The U.S. Federal Government	□	□	□	□	□
Traditional media such as newspapers or TV	□	□	□	□	□
U.S. technology companies such as Facebook, Apple, Amazon, Netflix, Google, or Microsoft	□	□	□	□	□

The next question asks about your political views.

26. Which of the following best describes your political views?

□ Very Liberal
□ Lean Liberal
□ Middle of the Road
□ Lean Conservative
□ Very Conservative
□ Other
□ Prefer not to say

END. Thank you for participating.

APPENDIX B

Survey Analytic Approach

This appendix describes details of the analytic approach to interpret the data from our survey of members of the American public. Weighted survey response data were obtained from ALP and analyzed within RStudio (Posit Software, 2022) using the statistical software language R (R Project, 2022) on an Apple MacBook Pro (Apple, 2022).

The survey response data were transformed for exploratory analysis. These transformations included correcting minor typos in the survey responses[1] and updating responses from text characters to ordinal factors. Exploratory analysis included calculating weighted summary tables for each survey response and weighted cross-tabulations of responses by specific demographic variables, including gender, age, and partisanship.[2]

After exploratory analysis, nonresponse (blank) responses and the response "prefer not to say" were found to be less than 0.3 percent and 2.7 percent of total responses, respectively. Therefore, both responses were omitted from further analysis.

After exploratory analysis, several demographic variables were created or revised to suit modeling needs with a reference category chosen for future regression modeling:

- age: Age values were grouped from a numeric value (in years) to the following categories:[3]
  - 18–30
  - 31–40
  - 41–50 (reference category)
  - 51–60
  - 61–74
  - 75+
- education: Education values were reduced from nine categories into three categories:[4]
  - high school or less

[1] For example, updating the response "Neither Agree or Disagree" to "Neither Agree nor Disagree."

[2] Tables were created using the pollster package, which calculates the design effect as described in Kish (1965, p. 257).

[3] Categories are consistent with the distributions used during weight construction of survey data (Pollard and Baird, 2017, p. 15).

[4] We used the same rationale as for the age variable; categories are consistent with distributions used during weight construction.

  - some college or bachelor's degree (reference category)
  - more than a bachelor's degree
- partisanship: Partisanship values were reduced from six categories (which distinguished levels of partisanship—e.g., "very liberal" versus "leans liberal") into four categories:
  - liberal
  - middle of the road (reference category)
  - conservative
  - other
- social media: Social media values were reduced from indicators of use for 13 social media sites (as listed below) into four categories of use:
  - mainstream only (reference category), which includes the following sites:
    - Facebook
    - Instagram
    - LinkedIn
    - Pinterest
    - TikTok
    - Twitter
    - WhatsApp
    - YouTube
    - Reddit
  - niche, which includes the following sites:
    - Parler
    - Truth Social
  - both mainstream and niche
  - none.

Regression analyses were performed to understand how demographic characteristics are associated with outcomes, such as trust and support of federal use of these technologies. Because we included such ambiguous response options as "Don't Know/It Depends" and such neutral responses as "Neither Agree nor Disagree" or "Neither Support nor Oppose," regression analyses included two phases. In the first phase, a regression[5] was initially performed on the outcome of if the response was "Don't Know/It Depends." This response type was then excluded from the data for a second regression,[6] using the same covariates as the first, for each outcome. Observations with missing outcome and covariate responses were omitted from both regressions. In the second phase, the "Don't Know/It Depends" and neutral responses

[5] Binominal generalized linear model (GLM) using the svyglm() function in the survey package in R.

[6] Ordinal logistic regression model using the svyolr() function in the survey package.

were grouped together and a regression[7] was performed on the outcome if the response was "Don't Know/It Depends" or neutral response or in the non–neutral response group.

To determine correlation of responses to different survey questions, a multistep process was used. Separate regressions[8] were performed on both survey questions of interest with the same covariates, excluding observations with missing outcome and covariate responses. Weighted correlations on the residuals of each regression were then produced.[9]

To determine whether responses to two questions were significantly different, responses were recoded as numbers.[10] The numeric difference between the responses to both questions was calculated for each respondent, omitting missing and "Don't Know/It Depends" responses. A regression model[11] with no covariates was then used to determine the average difference between responses to both questions, and statistical output was reported. This procedure was also repeated to assess differences between agreement responses and any other responses using the same method.

[7] Binominal GLM using the svyglm() function in the R package *survey*.

[8] Gaussian GLM using the svyglm() function in the R package *survey*.

[9] Using the wtd.cor() function in the R package *weights*.

[10] Labeling "strongly agree" as 1, "agree" as 2, "neither agree nor disagree" as 3, "disagree" as 4, and "strongly disagree" as 5.

[11] Gaussian GLM using the svyglm() function in the R package *survey*.

Abbreviations

ACLU	American Civil Liberties Union
AI	artificial intelligence
ALP	RAND American Life Panel
CBP	U.S. Customs and Border Protection
COVID-19	coronavirus disease 2019
DHS	U.S. Department of Homeland Security
FRT	face recognition technology
GAO	U.S. Government Accountability Office
GLM	generalized linear model
GPS	Global Positioning System
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
LPR	license plate reader
OMB	Office of Management and Budget
PII	personally identifiable information
PRA	Paperwork Reduction Act
S&T	Science and Technology Directorate
TSA	Transportation Security Administration
USSS	U.S. Secret Service

References

Access Now, Advocacy for Principled Action in Government, AFT Massachusetts, American Civil Liberties Union, American Library Association, American Muslim Empowerment Network, Amnesty International USA, Asian Americans Advancing Justice, Boston Public Library Professional Staff Association Local 4928 MLSA-AFT, Boston Teachers Union, Campaign for a Commercial-Free Childhood, CAIR Washington, Center for Constitutional Rights, Center on Privacy and Technology at Georgetown Law, CertNexus, Charles Hamilton Houston Institute for Race and Justice at Harvard Law School, Civil Liberties Defense Center, Climate Defense Project, Council on American–Islamic Relations, Defending Rights and Dissent, Densho, DesigniIT International aka KnowledgeHouseAfrica, Earthworks, Electronic Frontier Foundation, Electronic Privacy Information Center, Encode Justice, Fight for the Future, Free Press Action, Freedom House, Indivisible Plus Washington, John T. Williams Organizing Committee, Library Freedom Project, Massachusetts Pirate Party, National Association of Criminal Defense Lawyers, New America's Open Technology Institute, New England Library Association, OCA Asian Pacific American Advocates, Open the Government, Palestine Legal, Poligon Education Fund, Project on Government Oversight, Restore the Fourth, Surveillance Technology Oversight Project, South Asian Americans Leading Together, Freedom to Read Foundation, Leadership Conference on Civil and Human Rights, Welcome Project, Elsa Auerbach, Joy Buolamwini, and Isaac Kamola, "Civil-Rights Group Letter to President Biden Calling for Facial Recognition Ban," *Washington Post*, updated February 17, 2021.

ACLU—*See* American Civil Liberties Union.

Ahlers, Mike M., "TSA Removes Body Scanners Criticized as Too Revealing," CNN, updated May 30, 2013.

Aleaziz, Hamed, and Caroline Haskins, "DHS Authorities Are Buying Moment-by-Moment Geolocation Cellphone Data to Track People," *BuzzFeed News*, October 30, 2020.

American Civil Liberties Union, "Automatic License Plate Readers," webpage, undated. As of March 22, 2023:
https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers

Apple, macOS, version 12.5, July 20, 2022.

Boudreaux, Benjamin, Douglas Yeung, and Rachel Steratore, *The Department of Homeland Security's Use of Emerging Technologies: Why Public Perception Matters*, RAND Corporation, PE-A691-1, 2022. As of April 27, 2023:
https://www.rand.org/pubs/perspectives/PEA691-1.html

Buolamwini, Joy, and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, Vol. 81, 2018.

CBP—*See* U.S. Customs and Border Protection.

Center for Democracy and Technology, "Recognizing the Threats: Congress Must Impose a Moratorium on Law Enforcement Use of Facial Recognition Tech," October 14, 2021.

Cox, Joseph, "CBP Refuses to Tell Congress How It Is Tracking Americans Without a Warrant," *Motherboard*, October 23, 2020.

Daniels, Jeff, "Lie-Detecting Computer Kiosks Equipped with Artificial Intelligence Look Like the Future of Border Security," CNBC, updated May 15, 2018.

DHS—*See* U.S. Department of Homeland Security.

DHS AI strategy—*See* U.S. Department of Homeland Security, 2020.

Electronic Frontier Foundation, "Street-Level Surveillance," webpage, last updated August 28, 2017. As of March 22, 2023:
https://www.eff.org/pages/automated-license-plate-readers-alpr

Electronic Privacy Information Center, "Comments of the Electronic Privacy Information Center to U.S. Customs and Border Protection of the Department of Homeland Security," docket USCBP-2018-0045, April 11, 2019.

Fowler, Geoffrey A., "TSA Now Wants to Scan Your Face at Security. Here Are Your Rights," *Washington Post*, December 2, 2022.

Funk, Cary, "Key Findings About Americans' Confidence in Science and Their Views on Scientists' Role in Society," Pew Research Center, February 12, 2020.

GAO—*See* U.S. Government Accountability Office.

Gershgorn, Dave, "'Aggression Detection' Is Coming to Facial Recognition Cameras Around the World," OneZero, September 25, 2020.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT)*, Part 3: *Demographic Effects*, U.S. Department of Commerce, National Institute of Standards and Technology, NISTIR 8280, December 2019.

Halter, Nick, "Minneapolis Bans Police from Using Facial Recognition Tech," Axios Twin Cities, updated February 12, 2021.

Hao, Karen, "The Two-Year Fight to Stop Amazon from Selling Face Recognition to the Police," *MIT Technology Review*, June 12, 2020.

Harwell, Drew, "San Francisco Becomes First City in U.S. to Ban Facial-Recognition Software," *Washington Post*, May 14, 2019a.

Harwell, Drew, "Both Democrats and Republicans Blast Facial-Recognition Technology in a Rare Bipartisan Moment," *Washington Post*, May 22, 2019b.

Harwell, Drew, "FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches," *Washington Post*, July 7, 2019c.

Heikkilä, Melissa, "The Walls Are Closing in on Clearview AI," *MIT Technology Review*, May 24, 2022.

Hill, Kashmir, "Wrongfully Accused by an Algorithm," *New York Times*, June 24, 2020a.

Hill, Kashmir, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020b.

Hill, Kashmir, and Ryan Mac, "Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System," *New York Times*, November 2, 2021.

Horowitz, Michael C., Lauren Kahn, Julia Macdonald, and Jacquelyn Schneider, "COVID-19 and Public Support for Autonomous Technologies—Did the Pandemic Catalyze a World of Robots?" *PLoS ONE*, Vol. 17, No. 9, September 28, 2022.

ICE—*See* U.S. Immigration and Customs Enforcement.

Internal Revenue Service, "IRS Announces Transition Away from Use of Third-Party Verification Involving Facial Recognition," press release, IR-2022-27, February 7, 2022.

Johnson, Khari, “How Wrongful Arrests Based on AI Derailed 3 Men’s Lives,” *Wired*, March 7, 2022.

Kavanagh, Jennifer, Katherine Grace Carman, Maria DeYoreo, Nathan Chandler, and Lynn E. Davis, *The Drivers of Institutional Trust and Distrust: Exploring Components of Trustworthiness*, RAND Corporation, RR-A112-7, 2020. As of April 27, 2023:
https://www.rand.org/pubs/research_reports/RRA112-7.html

Kish, L., *Survey Sampling*, John Wiley and Sons, 1965.

Konkel, Frank, “Bipartisan Calls to Regulate Facial Recognition Tech Grow Louder,” Nextgov, July 14, 2021.

Kostka, Genia, Léa Steinacker, and Miriam Meckel, “Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States,” *Public Understanding of Science*, Vol. 30, No. 6, August 2021.

Lyons, Kim, “ICE Just Signed a Contract with Facial Recognition Company Clearview AI,” *The Verge*, updated August 14, 2020.

Marullo, Ross, Robert Casparro, Bhargav Patel, and Brenda Velasco-Lopez, *SMART: Social Media Analytics and Reporting Toolkit—Data Collection Report*, U.S. Department of Homeland Security, Science and Technology Directorate, RT-T-R-14, May 2020.

McKay, Tom, “Shady Face Recognition Firm Clearview AI Says It’s Left Canada amid Two Federal Investigations,” *Gizmodo*, July 6, 2020.

Miller, Maggie, “DHS Hacked as Part of Massive Cyberattack on Federal Agencies: Report,” *The Hill*, December 14, 2020.

Myers, Steven Lee, and Zolan Kanno-Youngs, “Partisan Fight Breaks Out over New Disinformation Board,” *New York Times*, May 2, 2022.

New York City Administrative Code; Title 22, Economic Affairs; Chapter 12, Biometric Identifier Information.

Ng, Alfred, “ICE Uses Database That Tracks License Plates, Raising Privacy Concerns,” CNET, March 13, 2019.

Office of Science and Technology Policy, White House, “Algorithmic Discrimination Protections,” webpage, undated. As of January 17, 2023:
https://www.whitehouse.gov/ostp/ai-bill-of-rights/algorithmic-discrimination-protections-2/

Paperwork Reduction Act—*See* Public Laws 96-511 and 104-13.

Peters, Jay, “IBM Will No Longer Offer, Develop, or Research Facial Recognition Technology,” *The Verge*, June 8, 2020.

Pew Research Center, “The American Trends Panel,” webpage, undated. As of January 18, 2023:
https://www.pewresearch.org/our-methods/u-s-surveys/the-american-trends-panel/

Pew Research Center, “Attitudes and Beliefs on Science and Technology Topics,” *Public and Scientists’ Views on Science and Society*, January 29, 2015a.

Pew Research Center, *Americans, Politics and Science Issues*, July 1, 2015b.

Pollard, Michael S., and Matthew D. Baird, *The RAND American Life Panel: Technical Description*, RAND Corporation, RR-1651, 2017. As of April 27, 2023:
https://www.rand.org/pubs/research_reports/RR1651.html

Pollina, Elvira, and Federico Maccioni, “Italy Outlaws Facial Recognition Tech, Except to Fight Crime,” Reuters, November 14, 2022.

Posit Software, RStudio, version 7872775e, July 22, 2022.

PRA—*See* Public Laws 96-511 and 104-13.

Public Law 93-579, Privacy Act of 1974, December 31, 1974.

Public Law 96-511, Paperwork Reduction Act of 1980, December 11, 1980.

Public Law 104-13, Paperwork Reduction Act of 1995, May 22, 1995.

Public Law 107-296, Homeland Security Act of 2002, November 25, 2002.

R Project, R, version 4.2.2, October 2022.

Rainie, Lee, Cary Funk, Monica Anderson, and Alec Tyson, *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns*, Pew Research Center, March 2022.

Rodrigo, Chris Mills, "Pressure Mounts on DHS to Stop Using Clearview AI Facial Recognition," *The Hill*, April 19, 2021.

Rudolph, Harrison, Laura M. Moy, and Alvaro M. Bedoya, "Not Ready for Takeoff: Face Scans at Airport Departure Gates," 2017. As of January 17, 2023: https://www.airportfacescans.com/

Sankin, Aaron, "Can I Opt Out of Facial Scans at the Airport?" 2020. As of January 17, 2023: https://themarkup.org/the-breakdown/2020/03/02/can-i-opt-out-of-facial-scans-at-the-airport

Science and Technology Directorate, U.S. Department of Homeland Security, "Automated License Plate Reader (ALPR)," fact sheet, January 5, 2021a.

Science and Technology Directorate, U.S. Department of Homeland Security, "Agency Information Collection Activities: Public Perceptions of Emerging Technologies," *Federal Register*, Vol. 86, No. 91, May 13, 2021b.

Science and Technology Directorate, U.S. Department of Homeland Security, "Public Perceptions of Emerging Technology," *Federal Register*, Vol. 86, No. 212, November 5, 2021c.

S&T—*See* Science and Technology Directorate.

Stellin, Susan, "Pat-Downs at Airports Prompt Complaints," *New York Times*, November 18, 2010.

Talla, Vasudha, "Documents Reveal ICE Using Driver Location Data from Local Police for Deportations," American Civil Liberties Union, March 13, 2019.

Tau, Byron, and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement," *Wall Street Journal*, February 7, 2020.

Transportation Security Administration, U.S. Department of Homeland Security, *Advanced Integrated Passenger and Baggage Screening Technologies: Fiscal Year 2019 Report to Congress*, January 14, 2020.

Transportation Security Administration, U.S. Department of Homeland Security, *Privacy Impact Assessment for the Travel Document Checker Automation Using Facial Identification*, DHS/TSA/PIA-046(d), November 17, 2022a.

Transportation Security Administration, U.S. Department of Homeland Security, "TSA Introduces State-of-the Art Identity Verification Technology at DEN Security Checkpoints," press release, November 18, 2022b.

TSA—*See* Transportation Security Administration.

Tyson, Alec, and Brian Kennedy, *Two-Thirds of Americans Think Government Should Do More on Climate*, Pew Research Center, June 23, 2020.

U.S. Code, Title 6, Domestic Security; Chapter 1, Homeland Security Organization; Subchapter III, Science and Technology in Support of Homeland Security; Section 185, Federally Funded Research and Development Centers.

U.S. Customs and Border Protection, U.S. Department of Homeland Security, *Privacy Impact Assessment for the CBP License Plate Reader Technology*, DHS/CBP/PIA-049(a), July 6, 2020.

U.S. Customs and Border Protection, U.S. Department of Homeland Security, "Global Entry: Trusted Traveler Program Enrollment," webpage, last modified January 3, 2023. As of April 27, 2023:
https://www.cbp.gov/travel/trusted-traveler-programs/global-entry

U.S. Department of Homeland Security, "Say Hello to the New Face of Speed, Security and Safety: Introducing Biometric Facial Comparison," webpage, undated. As of January 17, 2023:
https://biometrics.cbp.gov

U.S. Department of Homeland Security, "IT Program Assessment: CBP—Automated Targeting System (ATS) (2010)," c. 2010.

U.S. Department of Homeland Security, "Artificial Intelligence Strategy," December 3, 2020.

U.S. General Services Administration and Office of Management and Budget, "A Guide to the Paperwork Reduction Act," webpage, undated. As of January 18, 2023:
https://pra.digital.gov/

U.S. Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518, June 3, 2021.

U.S. Government Accountability Office, *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues*, GAO-22-106154, July 27, 2022.

U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services*, DHS/ICE/PIA-054, May 13, 2020.

U.S. Office of Personnel Management, "Cybersecurity Incidents," webpage, undated. As of January 18, 2023:
https://www.opm.gov/cybersecurity/cybersecurity-incidents/

U.S. Secret Service, U.S. Department of Homeland Security, *Privacy Impact Statement for the Facial Recognition Pilot*, DHS/USSS/PIA-024, November 26, 2018.

Vogels, Emily A., "Support for More Regulation of Tech Companies Has Declined in U.S., Especially Among Republicans," Pew Research Center, May 13, 2022.

Vogels, Emily A., and Andrew Perrin, "How Black Americans View the Use of Face Recognition Technology by Police," Pew Research Center, July 14, 2022.

Wang, Nina, Allison McDonald, Daniel Bateyko, and Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, Center on Privacy and Technology at Georgetown Law, May 10, 2022.

Artificial intelligence (AI) systems could be crucial in supporting the U.S. Department of Homeland Security's (DHS's) core missions. DHS already uses AI in homeland security missions, and it seeks to further integrate emerging AI capabilities in other applications across DHS components.

However, the full potential of DHS use of emerging AI technologies is subject to several constraints, one of which is how people view government use of those technologies. Public perception of government use of technology is important for several reasons, such as to establish trust in and legitimacy of the government, to facilitate necessary funding and legislative support from Congress, and to foster collaboration with technology companies and operational partners.

Some of these key stakeholders have raised concerns about DHS use of AI technologies, including risks that DHS applications violate privacy and civil liberties, exacerbate inequity, and lack appropriate oversight and other safeguards. These concerns could shape or restrict DHS use of technology, so it is important that DHS understand the extent to which the public agrees with the department's approach to addressing these concerns.

Researchers sought to evaluate public perception of the benefits and risks of DHS use of AI technologies. They developed a survey in 2020 with questions about current and planned DHS use of AI technologies, with a focus on four types of technologies: face recognition technology, license plate–reader technology, risk-assessment technology, and mobile phone location data. The survey was fielded using the RAND American Life Panel, a nationally representative panel of the American public.

$27.00

ISBN-10 197741124-X
ISBN-13 9781977411242

52700

9 781977 411242

Cover image: Adobe Stock/andreusK.
RR-A691-1