March 2022

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

BENJAMIN BOUDREAUX, DOUGLAS YEUNG, RACHEL STERATORE

The Department of Homeland Security's Use of Emerging Technologies

Why Public Perception Matters

The U.S. government frequently deploys emerging technologies that directly affect the American public. The U.S. Department of Homeland Security (DHS), for example, has recently deployed technologies that include artificial intelligence (AI) and machine learning (ML), such as face-recognition technology (FRT), fifth-generation (5G) network technology, counter–unmanned aircraft systems, and chemical and biological detection. Such technologies offer a variety of potential benefits, such as automating decisionmaking or processes to increase speed, accuracy, or convenience (West and Allen, 2018). There are also risks associated with the use of such technologies (Osoba and Welser, 2017), such as infringement of privacy and civil liberties (Yeung, Balebako, et al., 2020), biased or discriminatory results (Buolamwini and Gebru, 2018), and lack of transparency and oversight (Richardson, 2019).

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER
An FFRDC operated by the
RAND Corporation under
contract with DHS

Before these technologies are deployed, their use by government entities typically involves an extensive acquisition process intended to ensure, for example, that vendors are selected fairly, costs are reasonable, and the technology will work as intended (Halchin, 2021). These processes are essential elements of successful technology deployment.

Public perception is another essential element that can help identify risks and benefits of the use of technology and can inform multiple stages of the technology acquisition and deployment life cycle. However, it can be underappreciated in ways that undermine the effective and trustworthy use of the technology. For example, in 2009, the Transportation Security Administration (TSA) deployed full-body scanners at airport security checkpoints. To search for potential threats, a TSA officer monitoring a scanner could view a full-body image of the traveler inside the scanner. These scanners were met with strong public reaction, including concerns about potential privacy invasions, discrimination, and infringement of civil liberties. Within weeks, complaints "poured in" from the traveling public (Stellin, 2010). Some of these complaints reflected frustration from dealing with unexpected or unclear procedures, implying a failure to anticipate people's expectations and to provide needed information.

The body scanners also attracted scrutiny in the media and from public stakeholders, such as privacy-advocacy groups. Research about the new TSA security procedures, which included the body scanners, found that, in blogs on three major social media platforms written within a single week in November, more than half of all news links were about the security procedures, thereby making them the top trending topic on those platforms (Pew Research Center, 2010). In addition, the Electronic Privacy Information Center, a nonprofit focused on privacy and civil liberties, sued TSA over its use of the scanners, arguing that the scanners invaded privacy and that the public could not opt out (Electronic Privacy Information Center, undated).

In this and other cases, the resulting attention when the government has failed to account for public perceptions in technology deployments has had consequences both for the intended technology use and for government personnel who work with the public; this lack of public trust has implications for homeland security. One anonymous TSA worker, describing stress about scanning transgender and non–gender-conforming passengers, alluded to the impact of public perception on the TSA workers' day-to-day lives: "A lot of the traveling public already hate us . . . . [W]e don't want to offend people by [scanning them] wrong" (Waldron and Medina, 2019). Eventually, TSA removed 250 older scanners, leaving in use those scanners with privacy-protecting software (Ahlers, 2013). Although the manufacturer of the removed scanners paid to remove them, the U.S. government most likely shouldered additional costs, such as installing the scanners, training per-

Abbreviations

5G	fifth generation
ACLU	American Civil Liberties Union
AI	artificial intelligence
CBP	U.S. Customs and Border Protection
DHS	U.S. Department of Homeland Security
FRT	face-recognition technology
JAMRS	Joint Advertising, Market Research and Studies
ML	machine learning
MMA	mental-model approach
TSA	Transportation Security Administration

A variety of important stakeholders, including members of Congress, technology companies, state and local governments, and civil liberties advocates, have raised concerns about DHS's use of emerging technologies.

sonnel, and building more privacy-protecting processes. Moreover, the body-scanner controversy continues to resonate with the public and underscores the potential for long-term impacts and mistrust from failing to anticipate the public's views on technologies that the government might deploy.

The TSA body-scanner example also suggests some of the different types of stakeholders that might raise concerns about government deployments of technology and seek to shape or constrain DHS's use of such technologies in other contexts. Researchers in academia or nonprofits might, for example, discover that technologies cause harms disproportionately to certain groups of people or are not as effective as claimed. Advocacy groups might also criticize the potential privacy violations of the broad surveillance that these government technologies enable. Local, state, or federal legislators might seek to limit the scope of technology deployments in their jurisdictions or restrict funding for these use cases. In addition, a variety of operational partners—including the private-sector companies that build many of the tools and state, local, federal, and international governments—might themselves have concerns that will need to be addressed.

DHS has several broad use cases of emerging technologies, for which the implementation could be affected by public perception. Examples of these DHS use cases of emerging technologies are

- **FRT**, which uses computers to match a face in a photo or video to a face in a database (DHS, 2020)
- **risk-assessment tools** that use computerized algorithms to assess how likely it is that something will occur (DHS, 2017)
- **license plate–reader technology** that uses computers to identify or match a license plate (or car tag) from a state-run database (DHS, 2021)
- **cell phone location tracking** that uses cell phone location data to track movements (Tau and Hackman, 2020).

Among the serious challenges DHS faces is misinformation about the current and planned use of emerging technologies and how this misinformation might influence public perception (Andrews, 2020). For example, DHS has already begun preparing to combat potential attacks against 5G cell towers that are based on false beliefs that 5G wireless technology causes coronavirus disease 2019

Americans have expressed concerns about how the government and private companies use people's personal data.

(COVID-19) (Nakashima, 2020). Misinformation could play a similar role in shaping public perceptions of other technology deployments, which might increase public scrutiny in ways that diminish the effective use of those technologies.

This Perspective (1) explores the ways in which public perception can influence the success of government technology deployments, (2) identifies different methods of assessing public perception, and (3) suggests ways in which government agencies, such as DHS, might account for public perception across the technology deployment life cycle. To begin, it first presents the nature of public perceptions, especially toward science and technology.

Public Perceptions of Government Use of Science and Technology

The term *public perception* can be difficult to define, but it includes both cognitive and affective, or emotionally driven, components across a wide variety of groups and stakeholders (Slovic et al., 2013; Kahneman and Frederick, 2002, p. 81; Tversky and Kahneman, 1974). Perception involves issue-specific knowledge, cognitive processes, beliefs, and feelings that drive how people experience the world around them and make decisions. Perception is important to understand across distinct *public* groups (for example, U.S. citizens over 18, people living in a particular area, or members of a racial or ethnic minority group), as well as *stakeholder* groups (for example, all levels of government, technology developers, academic researchers, international partners, and advocacy groups). For instance, public perception of government use of technology involves what someone from a specific group knows about a technology and how the government uses it, as well as how someone feels about the technology itself and the circumstances surrounding its use.

In general, research suggests that public confidence in science remains high (Funk and Kennedy, 2020) but that there is skepticism about transparency and accountability in how scientific work is conducted (Funk, 2020). Even since the initial crisis of the COVID-19 pandemic, confidence in science remains higher than in other institutions, although it has declined modestly among all Americans (Jones, 2021). Other research underscores an overall decline in trust in basic facts across various institutions in American society (Kavanagh and Rich, 2018). Some recent polling suggests that the American public's views on government use of technology might be shaped by people's views of the specific type of technology and the institution deploying it. At the broadest level, that polling also suggests that Americans generally distrust the government (Rainie, Keeter, and Perrin, 2019). A 2021 public survey by Edelman showed that the public's trust in the technology sector has declined in the past decade and even in the past year (Edelman, 2021). Perhaps as a result, Americans have also expressed concerns about how the government and private companies use people's personal data (Auxier et al., 2019), which is a key feature of many technology deployments.

Another important factor that might affect public perception is the type of technology being deployed and the extent to which the public might have direct contact with it. For instance, some people might favor a government role in supporting technology to address large-scale challenges, such as climate (Tyson and Kennedy, 2020). In surveys, people are also more positive about relatively abstract science and technology areas, such as space exploration and bioengineering, and are split or more negative about areas that might affect them personally, such as brain implants or genetically modified food (Pew Research Center, 2015).

Public perception might also shift based on the content of what is being asked and the timing and mode of collecting information. The public might not always have a well-defined view of new technologies or the many ways the government uses them. In some cases, the public might have a defined and hardened view about a specific technology but not have clarity on the details of how DHS uses it and the potential safeguards that are in place for addressing harms. Many advanced technologies—especially AI and ML—are "black boxes" that operate in ways that might be highly opaque to the public and perhaps even to DHS operators themselves (Bleicher, 2017). Moreover, public perception in different communities might shift as these technologies become widespread or more (or less) well-understood.

Ultimately, the uncertainty and potentially shifting landscape related to the public's views underscore the importance of a routine and comprehensive approach to better understanding public perception, including current views about key technologies and the socioeconomic, demographic, and other factors that correlate with different attitudes.

How Public Perception Can Affect Technology Deployment

The ultimate objective of DHS uses of technology is to promote American safety and security, per its mission statement: "[DHS] will safeguard the American people, our homeland, and our values" (DHS, 2019b). Whether DHS deployment of emerging technology will meet this objective will depend in part on the public's support of its use.

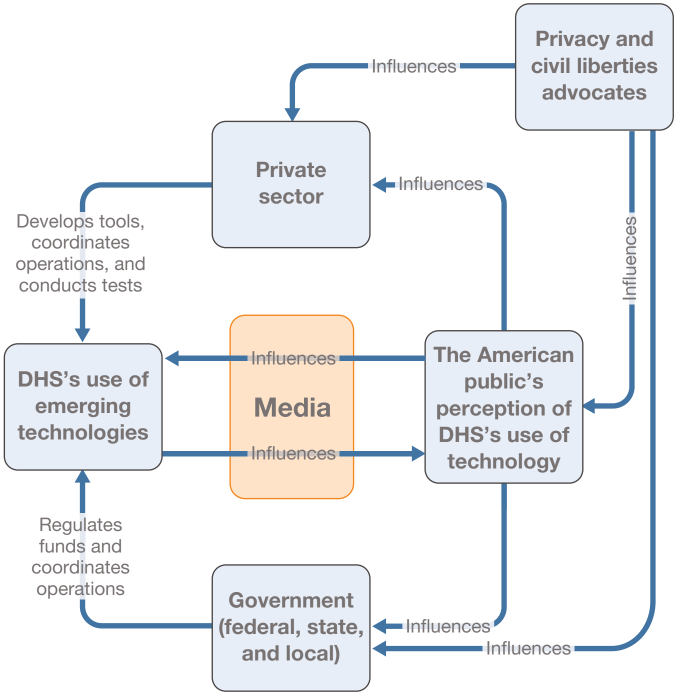
A variety of stakeholders have raised concerns about the harmful implications of technologies, such as FRTs, and have sought public support for legislative and other action to regulate and shape how they are deployed. Some of the stakeholders that have engaged in this discussion are federal, state, and local governments; private-sector technology developers; academic researchers; international partners; and civil rights advocacy groups. Each of these actors can play an important role in shaping DHS's use of emerging technology, and the issues they raise might inform or influence public perception in ways that could either further fuel public alarm or help to build public trust and support.

The mapping in the figure depicts the key stakeholders that are concerned about public perception and their differing roles and relationships with DHS's use of technology. As depicted in the figure, these actors have levers available to them that might enable or constrain DHS's ability to implement technology.

This diagram helps illustrate three major reasons that understanding public perception matters to DHS:

- to build public trust and promote public uptake of technology uses
- to be prepared for potential regulatory and funding decisions
- to promote key partnerships.

Mapping of DHS's Use of Technology and the Importance of Public Perception


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

Each of these three considerations directly relates to DHS's ability to use technologies that protect the public and improve homeland security. Before we discuss these three reasons in more detail, we note that one element of this mapping merits a bit of discussion: the role of different forms of media in reporting on the use of technology.

The media play a role in shaping how the public thinks, but the ways in which the media operate as a source of information that conditions public attitudes is highly complex.[1] For instance, there is a body of research that explains the "virality" of content circulated through both social media and traditional media (Berger and Milkman, 2012; Tellis et al., 2019). In many cases, the public tends to engage more strongly with certain types of content—such as stories that provoke an emotional reaction or information that confirms existing views (see, for instance, Tellis et al., 2019). This effect might increase the salience of content describing acts that DHS seeks to prevent, such as terrorism. It might also increase the public salience of technology failures, such as when someone is wrongfully arrested because of biased FRT (Hill, 2020).

Beyond traditional and social media, an additional source that might affect public perception is depictions of technology in fictional narratives, such as science fiction films. For the sake of a compelling story, these presentations might exaggerate the drawbacks of technologies without accounting for the more-benign benefits they might offer or vice versa, thus influencing perceptions negatively or positively. Media consumption might influence both the information that the public has about technology and the public's opinions about appropriate use.

Trust and Public Uptake

A primary reason public perception matters to DHS is so that the department can ensure that it is using technologies in the ways that most effectively build public support and trust. Arguably, this is part of preserving American values and undergirds the legitimacy of a democratic government by and for the people. It also helps ensure that the public judges that the specific use is appropriate, just, and fair. Importantly, the issue of public trust also relates to DHS's ability to improve homeland security because, if people do not have sufficient trust in DHS's uses of emerging technologies, they might try to circumvent such uses.

A better understanding of public perception can reveal when specific communities—especially marginalized or underrepresented communities—have concerns that are otherwise not given sufficient attention in mainstream discourse. President Joe Biden's "Executive Order on Advancing Racial Equity" notes that "entrenched disparities in our laws and public policies, and in our public and private institutions, have often denied . . . equal opportunity to individuals and communities" (Biden, 2021). In order to ensure the full inclusion and participation of all communities, especially of historically marginalized groups, it will be important to better understand these groups' perspectives and concerns. DHS's mission to safeguard the American public will be significantly enhanced with *all* Americans' trust and support for its mission. To put it simply, public perception matters to DHS because DHS serves the public.

> If people do not support a specific use case, they might resist using the technology, thereby undermining the goals of deploying it in the first place.

In seeking to build public trust, it will be valuable for DHS to distinguish attitudes about the U.S. government in general, attitudes about DHS and its components (e.g., TSA, U.S. Customs and Border Protection [CBP]), and attitudes about the specific emerging technologies under consideration. For instance, even as Americans become more comfortable using face recognition to unlock their phones or while traveling, that comfort level might not imply similar levels of comfort with FRT in other contexts, such as at protests or voting locations. It will be important to clearly understand these distinctions to most effectively understand where trust and public support might be lacking and thus how it can be built.

In addition, in some use cases, the public has a clear, voluntary choice in whether to participate in a program that claims to offer increased convenience, accuracy, or security. In these cases, views about DHS uses will matter for people's decisions about whether to participate in DHS programs. If people do not support a specific use case—for instance, because of a belief that it violates privacy unnecessarily or is disproportionately cumbersome relative to its benefit—they might resist using the technology, thereby undermining the goals of deploying it in the first place.

If usage data are an indicator of public support, some specific DHS uses of technologies seem to be the subject of increased public support, such as CBP's use of FRT through Trusted Traveler programs (e.g., Global Entry) (CBP, 2021). This observed behavior is one way to gauge public support, but only when the technology is truly opt-in and the opportunity costs for alternative actions are low—which might be relatively rare. That said, tracking these public decisions and getting more detail on why the decisions were made will be important for DHS to implement programs with broad public uptake.

There is not yet new federal law that applies to many of the AI, ML, and other emerging technologies that have recently been developed or that applies to how DHS can use these technologies.

Preparing for Legislation and Securing Funding

Additional reasons to care about public perception are to anticipate potential legislation and to ensure that the concerns of elected officials and government regulators are addressed in technology deployments. Legislators can legally constrain or even prohibit DHS's use of a technology, so understanding the views of their constituents can help DHS be prepared for attention and inquiries from Capitol Hill and from state and local governments.

Although longstanding federal law and constitutional protections apply to DHS activity writ large, there is not yet new federal law that applies to many of the AI, ML, and other emerging technologies that have recently been developed or that applies to how DHS can use these technologies. That said, some federal, state, and local governments have taken an increased interest in how government actors deploy technology, especially face recognition and other AI tools. This development comes in the context of the public's declining trust in the technology sector, which might increase constituents' desire for government regulators to take action (Edelman, 2021).

Congressional committees have held hearings that provide opportunities for advocacy groups and researchers to shape how lawmakers think about the harmful implications of technology. For instance, these groups have brought congressional attention to concerns about discrimination and inequity in the use of AI surveillance systems

(Committee on Oversight and Reform, 2019). As described in these hearings, discrimination and inequity might be due to characteristics of AI systems, such as dependence on training data that are biased or unrepresentative, or biases programmed directly into the optimization function of AI models. Harmful discrimination can also result from using accurate technologies in contexts of historical inequity—such as the use of predictive policing or recidivism risk–assessment algorithms that are optimized for accuracy yet have a greater error rate for certain minority groups because of historical disparities in arrest rates (see Yeung, Khan, et al., 2021).[2]

Congressional hearings have also raised questions about privacy risks of surveillance technologies, the limited transparency about the quality of the technologies, and the implications for how they are used. Congress has also posed specific questions to DHS officials—for example, more than 20 members of Congress presented a series of critical questions to DHS about CBP's use of face recognition (Wild et al., 2019)—and a better understanding of public perception will help DHS respond to these and other inquiries.

In addition to hearings, several bills have been proposed that would prohibit or restrict the use of face recognition and other biometric technology by federal law enforcement, including DHS.[3] The American Civil Liberties Union (ACLU) and more than 60 other privacy and faith groups have written an open letter to Congress to push for a moratorium on the federal government's use of FRT (ACLU, 2019). As these discussions continue, it will be valuable for DHS to understand the views of the public so it can be prepared to present its perspective effectively to Congress, explain its current and planned use of technologies, including how the technologies would support DHS's safeguarding mission, take precautions or decide to limit technology use, and shape possible legislation in line with the public interest.

In state and local governments, recent years have seen increased legislative action, and some states have already enacted laws that apply to local government use of technologies, including face recognition.[4] Although these various state and local efforts do not apply directly to federal actors, they have implications for federal use. Constituents might themselves support state or local restrictions, so a divergence between local restrictions and expansive use at the federal level might lead constituents to mistrust the federal actors and fuel objections.

In addition, bans or restrictions by state governments will have ramifications for the private-sector partners that develop and furnish technological tools. For instance, in order to comply with the Illinois Biometric Information Privacy Act (740 ILCS 14), the FRT company Clearview AI removed all Illinois residents from its face-recognition database, which both makes the database less useful for federal law enforcement and raises questions about whether other states will follow (Hill, 2021b).[5]

In the context of all of this legislative attention, a better understanding of public perception can help DHS predict what legislation might be on the horizon that would affect how—or whether—it uses certain technologies. It can also help DHS explain to Congress and to state and local governments how it is meeting the most-fundamental concerns about implications for privacy, bias, transparency, and other issues as they are raised.

In addition, Congress maintains the power of the purse to provide DHS with the funds it needs to acquire technologies and to implement programs. If there is less public support—for instance, if constituents express serious concerns about specific uses—Congress might reduce or cancel funding. Here again, understanding such concerns can help DHS better engage Congress to ensure that the department can be prepared for and anticipate funding decisions and work to secure the funding it needs to best safeguard the American public and build trust and support.

Strengthening Partnerships

A third reason that public perception matters for DHS is to build and strengthen its partnerships that are essential for promoting homeland security. To use technology effectively, DHS depends on a variety of partners that are themselves subject to public pressure from their customers, shareholders, and employees. Some of DHS's partnerships for emerging-technology deployments are nascent and might even be fragile because of the power of public perception in influencing companies' behavior. A better understanding of public perception could help DHS strengthen these relationships and maintain one of DHS's core values, "honoring our partners" (DHS, 2019a).

Technology developers provide the basic tools that DHS seeks to use, and the private sector is an important source of technology, especially for advanced AI systems. In addition, DHS has operational relationships with partners, such as law enforcement, across federal, state, and local governments that are important for effective collaboration. It also maintains partnerships with transportation authorities both domestically and internationally—for instance, the foreign governments that participate in Trusted Traveler programs (CBP, 2021). Last, researchers and standard-setting organizations partner with DHS to ensure that technologies meet appropriate standards and otherwise develop and refine technology for operational use.[6] Without these relationships, DHS might not have access to the advanced technology it seeks to use or have the operational arrangements to use it effectively, thereby hindering DHS's homeland security objectives.

> Some technology developers in the private sector have expressed concern about government use of certain technologies; in some high-profile cases, important private-sector actors have decided not to partner with DHS because of public concerns.

Some technology developers in the private sector have expressed concern about government use of certain technologies, in part because of public outcry about their use. And in some high-profile cases, important private-sector actors have decided not to partner with DHS because of public concerns. For instance, employees and shareholders of major firms have demanded that the companies not sell face recognition to police or government agencies, especially for law or immigration enforcement (see, e.g., Vincent, 2018; ACLU, 2018; and Dave, 2020). Several companies have stopped selling FRT to governments altogether (IBM, 2020) or until Congress passes a face-recognition law that would establish privacy and ethical standards (Amazon, 2020; Greene, 2020; Ovide, 2021). As stated by one major technology company, "now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies" (IBM, 2020). In addition, Axon, one of the largest suppliers of law enforcement technology, such as body cameras, has decided not to sell FRT to law enforcement, in part because of the critical questions raised by its ethics board (Smith, 2019).

The private sector is diverse, and other companies, including Clearview AI and NEC Corporation, have continued to sell AI and FRTs to government, and there are media reports that Clearview AI has signed a contract with U.S. Immigration and Customs Enforcement (Lyons, 2020). However, that company has been under significant scrutiny both in the United States and internationally and is subject to multiple litigation challenges, and its data-harvesting practices have even been deemed illegal in Canada, a significant operational partner (Hill, 2021a). Many of these private-sector partners find themselves under increasing public scrutiny, which will have ramifications for how DHS can leverage some of its advanced tools.

International governments are also increasingly turning their attention to AI and other emerging technologies and are moving quickly to implement regulations that might have implications for U.S. public perception and DHS collaboration. The European Union, for example, has proposed a set of regulations that would significantly constrain key technologies—for instance, it has proposed broad prohibitions on the use of real-time biometric identification (such as face recognition) in public places for law enforcement purposes (European Commission, 2021). Although it is not clear how these kinds of regulations will affect operational relationships with DHS, they do indicate how the international community is thinking about these technologies and how this might increase pressure on the U.S. government to develop its own regulations.[7]

To best secure and strengthen its partnerships, DHS will need to ensure that it uses technology in ways that the partners, influenced by the public at large, will continue to support. To better understand this dynamic, as well as the broader factors associated with public attitudes, DHS can proceed in any of a multitude of ways, which we address in the next section.

How to Assess Public Perception

DHS could benefit from reliable indicators of public perception, as well as an understanding of the factors that affect public trust, using affordable methods for capturing and interpreting such indicators within reasonably short time frames. Yet perceptions are intangible and multidimensional—made up of, and driven by, various conditions. Adding to this complexity is that public perception about emerging technology is a shifting terrain. Together, these considerations make it difficult for DHS to identify public views that might be relevant.

Public-perception studies rely on imperfect indicators and methods to describe views on topics of interest at a single point in time. How these views are tapped depends on the research objectives and communities of interest. Herein lies the power of the research design. By design, research can focus on the perceptions of different communities based on social, economic, demographic, or organizational characteristics, and group composition can be altered to maximize insights into how similar people communicate in natural settings or to include diverse perspectives to explore differences between them.

Perceptions can be either *elicited* or *observed*. Surveys, interviews, and focus groups (e.g., with members of the public, stakeholders, or experts) are all examples of elicited methods, whereby the participant is provided prompts in various settings and formats to elicit a response. Observed methods include content analysis (e.g., social media analysis of perceptions on Twitter), behavioral observations (e.g., voting or internet search behavior), literature reviews, and secondary data analysis that use existing data in naturalistic settings—in other words, analysis on data not derived from a specific prompt posed by a researcher. Many collection methods might consider the influence of the Hawthorne effect—that is, the potential change in behavior when someone is aware of being under observation (McCarney et al., 2007). Table 1 summarizes a subset of these approaches, offering other considerations for their use.

Elicited Methods

Interviews

An interview typically involves questions on a topic of interest posed by an interviewer to an individual. Interviews can foster in-depth exploration of public perceptions, insights from experts (e.g., through expert interviews and panels), or stakeholder input. DHS might use interviews to explore mental models—individuals' internal representations of external reality, which play a major role in cognition, reasoning, and decisionmaking—of emerging technologies (Morgan et al., 2002). Certain interviews offer the opportunity to ask respondents to clarify or expand on specific points, so these types of interviews can reveal far more-complex attitudes than surveys can. Interviews allow deeper access to the ways in which knowledge and opinions are internalized, encoded, and expressed in one's natural language—thus supporting a sophisticated understanding of perceptions. However, interviews can be resource intensive, and findings cannot be generalized to a larger population, a fact that can pose challenges when the objective is to understand overall public views that might be of interest to DHS. As an example of this approach, interviews with community members might be useful when DHS wants to understand the nuance of FRT deployment surrounding a sensitive government building.

Focus Groups

Focus groups typically convene six to 12 people who are representative of the target group whose perceptions are of interest. A facilitator might lead participants through a protocol (i.e., a carefully planned line of questioning)

TABLE 1

Select Methods for Assessing Public Perceptions

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 6–12 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 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	Data collection 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

[a] Elicited methods might be subject to the requirements of the Paperwork Reduction Act (Pub. L. 104-13, 1995), a federal law mandating certain authorizations from the Office of Management and Budget 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.

and can observe how perceptions are communicated, exchanged, reinforced, and dispelled in a social, interactive setting. One example of how focus groups might be used is to understand a specific marginalized group's views on risk-assessment systems that might have a disparate impact or error rate on them.

Research that uses focus groups can strike a good balance between depth and breadth. However, focus groups are also subject to conforming concerns (i.e., biasing toward group consensus). Although administering a focus group is generally inexpensive, focus group findings have little basis for empirical generalization. Conversely, focus groups can offer conceptual or theoretical generalization to inform subsequent, confirmatory surveys. Like with individual interviews, research using focus groups should include tested protocols, facilitator training, and qualification of reported results. Protocols should include probes that specifically mitigate conforming concerns (e.g., “Does anyone have a different perspective on this issue?” or “Have we missed anything important in this discussion?”).

Surveys

Surveys are a means of gauging public attitudes on a particular topic, such as people’s perceptions of emerging technologies or environmental risks. Conducting surveys allows researchers to elicit subjective opinions from a sample of interest and to perform analyses to describe patterns or infer something about the study population that the sample represents. For example, a large nationwide survey could help compare public views on license plate readers that rely on vehicle databases that vary across states.

Methods for survey studies depend on their intended purpose and involve different types, designs, questions, and response options. Sampling approaches, sources of bias, adherence to reporting standards, and the survey instrument itself are all important in ensuring study quality. Within a given type of survey design, different options include the time period, respondent group, variable choice, data collection method, and analytical approach. This discussion is bounded to two survey options: closed form and signal-detection design.

The closed-form survey employs the most-common response scales (e.g., multiple choice, dichotomous, rating, Likert). Because surveys are such a common part of everyday life, the closed-form approach offers a familiar format—and perhaps a degree of comfort—to respondents. The question format provides relatively clear expectations and less variance than other types of surveys do. However, this can also be a disadvantage. If the research objective is to capture the full range of beliefs or attitudes about a topic, the closed-form option might dilute certain perspectives that would be important for measuring public perceptions.

A signal-detection design is based on signal-detection theory (Macmillan and Creelman, 2004) and can be employed to determine the degree to which diverse publics accept various emerging technologies to identify people’s decision thresholds and turning points. This option requires careful consideration of public participants, as well as thorough pretesting and logical design in congruence with signal-detection theory. Although inherently more complex than closed-form survey methods, this option provides quantitative data for each respondent, which is more robust for certain statistical tests. The approach offers unique insight into the direct response biases in respondents’ acceptance of certain scenarios, decision thresholds, and turning points. These metrics are calculated consistently across participants to allow direct and between-group comparisons (e.g., if researchers are interested in the predictive power of certain characteristics for a group’s risk acceptance for various technologies).

Some Considerations for Eliciting Public Perceptions

Perceptions are influenced by cognitive and affective biases (Kahneman and Frederick, 2002, p. 81; Haselton, Nettle, and Andrews, 2015; Johnson and Fowler, 2011).[8] *Cognitive bias* refers to a distortion in human cognition compared to some aspect of objective reality (Haselton, Nettle, and Andrews, 2015), while affective biases are emotion based. An example of a much larger set of cognitive biases is *availability* (Tversky and Kahneman, 1974), or the tendency to overestimate the probability of events that are similar to easy-to-recall events. For instance, future emerging technologies might be viewed as more likely to be discriminatory because of recent experiences of racial bias in the use of FRT. The *affect* heuristic is an example of an emotional shortcut used to make decisions (Slovic et al., 2007). For all collection methods, both cognitive and affective biases require careful attention, as well as trained interviewers or facilitators (for focus groups) to proactively mitigate these biases. An example is to use a funnel design, which is a best practice to mitigate priming effects, by posing broad questions of interest first, followed by more-specific probes. Priming effects can occur when exposure to initial questions could subconsciously influence responses to later questions. In addition, questions should undergo extensive pilot testing for comprehension (i.e., questions are not only understood but also interpreted the way they were intended to be). Protocol designs that build in pretests and mitigations against biases help ensure the integrity of the research method, improving the validity and trustworthiness of the findings. Researchers must also provide guidance about how to interpret or qualify the results, considering the elicitation method used.

Observed Methods

Content Analysis

Content analysis is a dual qualitative and quantitative approach. Text data are classified or "tagged" qualitatively based on the presence or absence of a particular word, concept, or theme. The objective is to formulate text (e.g., documents, media, transcripts) into "data" for structured, quantitative analysis. Potential themes are identified, categorized, and organized based on a set of rules or criteria. Safety, privacy, and consent are potential themes related to emerging technologies. Safety subthemes, for instance, could include the probability of harm and the severity of a potential consequence.

Content analysis can be performed manually by trained coders, semiautomatically, or automatically using coding or data-processing software. RAND-Lex—a suite of natural-language processing tools capable of scanning millions of lines of text to identify what people are talking about, how they fit into communities, and how they see the world—is one such example. Another example is the Linguistic Inquiry and Word Count text analysis tool, which sorts words into predefined psychological categories, such as emotion (Pennebaker, Booth, and Francis, undated). Emotions and attitudes that are expressed can then be linked to topics of discussion or real-world events to suggest attitudes about those topics and events. This tool can be used for content analysis of public attitudes expressed in online media (Yeung, Elson, et al., 2012). Linguistic Inquiry and Word Count has recently been used to analyze the mental states of mass shooters (Hammarlund et al., 2020, p. 225) and perceptions of risk during the COVID-19 pandemic (Dyer and Kolic, 2020).

Behavioral Observations

Behavioral observations can help researchers understand public perceptions based on how people act in either natural or controlled settings. Certain behavioral observation methods might be particularly useful for DHS to consider. Web searches provide one such opportunity to observe people's interest in a topic through their actions online. Because people directly search for information, web searches do not contain the same biases that might exist on social media, where people might choose to present themselves in particular ways. Web search data can be aggregated to explore interest in specific topics, such as face recognition or other emerging technologies, over time or in specific regions. This allows comparison between groups or examination of how events can influence trends in searches. Another specific benefit of web searches is that they can reveal sensitive concerns that might be difficult to elicit. For example, during the Great Recession, some searches, such as "my dad hit me," seemed to increase in areas where child services had been cut (Stephens-Davidowitz, 2013). As an example of web search analysis, DHS might analyze web searches to understand shifts in extremist viewpoints and whether they are linked to interest in violent action, or it might use search data to monitor population needs in case of disaster.

Another potentially useful approach is multidimensional scaling, which is a way to spatially represent nonmetric data, such as ranked preferences for different emerging technologies, with a small number of parameters (Baird and Noma, 1978, pp. 177–205). Multidimensional scaling can be approached as an analysis tool or as a psychological model; these methods can be used to observe dimensions on which people sort technologies. For example, dimensions might include efficiency, fairness, and familiarity with a technology. The advantage of this method is that the dimensions emerge from the sorting behavior and do not require respondents to generate verbal descriptions of dimensions of which they might not be aware. DHS might leverage multidimensional scaling to evaluate how these dimensions respectively influence someone's comfort level in, say, the use of license plate–reader technology. Interpretation of dimensions should be handled with care, understanding that the meaning might not uncover any useful, underlying structure. In addition, any process to reduce the number of data parameters or dimensions is accompanied by a loss of information.

Other behavioral observation methods could also prove useful, such as analyses of voting behaviors or market research to gather consumer preferences. DHS's acquisition process already accommodates market research for vendor selection (DHS, 2009), which could be expanded to explicitly consider public perceptions. As a model, DHS could look to how the U.S. Department of Defense's Joint Advertising, Market Research and Studies (JAMRS) conducts market research "to explore the perceptions, beliefs, and attitudes of American youth as they relate to joining the Military" (JAMRS, undated). For instance, JAMRS regularly surveys and reports on significant influences (e.g., friends who served in the military) on youth attitudes and what might increase positive perceptions about the military.

Combining Methods

Note that these methods need not be used independently. The power of these methods is strengthened when they are used in concert. One example of a hybrid approach is the mental-model approach (MMA), which aims to close critical gaps between the knowledge that people need in order to make and implement sound decisions and the knowledge they already have (Morgan et al., 2002). The MMA is designed to elicit people's perspectives on topics in their natural formulation through an initial set of interviews followed by a larger confirmatory survey, providing a more robust picture of public perceptions than any one method alone (Bruine de Bruin and Bostrom, 2013). The MMA can reveal common misconceptions and knowledge gaps to target in official DHS messages and communications. Structured, defensible methods, such as the MMA, help build trust not only in the message itself but also in DHS.

Opportunities for DHS to Understand and Integrate Public Perception in Technology Acquisition and Deployment

There could be significant benefits from integrating advanced technology for DHS missions, but these benefits might not be realized if the public is not sufficiently supportive. TSA's experience with body scanners illustrates the importance of anticipating and planning for the public's response to technology deployments. As this Perspective has noted, the public consists of a variety of distinct groups, and different demographic and other factors might correlate with different attitudes across these groups. These public attitudes will have an influence on the stakeholders that play different yet crucial roles in enabling DHS use of technology, such as stakeholders that provide technical tools or act as operational partners. Public concerns might also lead these actors to restrict, prohibit, or otherwise challenge DHS's use of technology by developing regulations, restricting funding, or declining partnerships. DHS could consider pursuing several opportunities to understand and integrate public perception in technology acquisition and development.

First, DHS could use public-perception methods to better understand specific communities' views and potential behavioral and emotional reactions to technology use cases. These methods would help to identify the attitudes held by different demographic groups and to understand some of the key associated factors, including age, gender, race, income, education, media consumption, political ideology, and use of technology. Questions that might be explored in public-perception studies include how different types of information sources (such as social media and traditional media sources) condition public attitudes in different communities. This approach could also help DHS better understand when a certain perspective is based on misinformation or is tied to a conspiracy theory (such as appears to be the case for 5G technology) so that DHS can more effectively engage and present accurate information.

Second, DHS could use public-perception methods to disaggregate attitudes about different elements of technology use cases. As noted above, a DHS use case of technology includes a DHS component (e.g., CBP), a specific technology (e.g., face recognition), and a specific purpose and context (e.g., border security at land crossings). The methods described in this Perspective could help to control for and distinguish these different elements to better understand where concerns are centered (e.g., on the technology or on the purpose and context) and where information might be lacking. These individual elements can also be further broken down: Even for a given technology, there might be some practices that are more controversial—for instance, using social media photos in face-recognition databases. And perception techniques would also enable DHS to distinguish different kinds of purposes or contexts in which the technologies will be used. This disaggregated detail would help DHS understand the landscape of its use of technology that will help inform risk mitigations and messaging.

Third, DHS could use public perception to inform preventive steps to address important concerns. This would involve using the information gathered about public perception to integrate pre- and postdeployment best practices into DHS use cases to build or maintain trust and support. In certain extreme circumstances, this might mean not using certain technologies or using them only with very clear restrictions or oversight mechanisms. More generally, it would provide a set of considerations that DHS could regularly integrate into cost–benefit analysis as it decides whether and how to deploy the technology.

Fourth, DHS could use public-perception information to better explain in its strategic communications how it is using technology to further its safeguarding mission. As noted above, this might include tailoring key strategic communications to different communities about the purposes of the use case (including the key benefits), correcting misunderstandings (including those fueled by misinformation and disinformation campaigns), and explaining the types of mitigations that address concerns. Specific messaging would also help with responses to Congress, privacy and civil liberties advocates, and operational partners. This is an opportunity for DHS to be publicly engaged and transparent in ways that could increase legitimacy and build public trust.

Operationalizing Public Perception in Technology Acquisition and Deployment

To make these observations more actionable and integrative, we have categorized them according to a notional technology acquisition and deployment framework that spans the technology's life cycle. The Perspective borrows the technology acquisition framework from RAND work on mitigating bias in law enforcement use of AI and ML systems (Yeung, Khan, et al., 2021). Just as harmful bias might enter into DHS use cases at different steps in the acquisition process, so can other issues that might be of concern to the public. In Table 2, we have indicated select ways to integrate public perception at these different stages.

For DHS to carry out its mission, the department will likely need to both field emerging technologies and effectively engage the public. The details of these activities will depend on the specific technology use cases. But across all cases of emerging-technology deployment, DHS will need to continue to effectively identify, evaluate, and engage with public perception in order to use emerging technologies effectively.

TABLE 2

Select Ways to Integrate Public Perception into a Notional Technology Acquisition and Deployment Framework

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).

Notes

[1] We thank our RAND Corporation colleague Keller Scholl for pointing out this important element. For the classic analytical approach to how public perceptions of risk are attenuated and amplified by cultural and institutional dynamics (such as the role of media), see Kasperson et al., 1988.

[2] For one example, see the debates about the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) recidivism risk algorithm discussed in Osoba, Boudreaux, et al., 2019.

[3] For instance, bills proposed in 2020 alone include the George Floyd Justice in Policing Act of 2020 (U.S. House of Representatives, 2020), the Facial Recognition and Biometric Technology Moratorium Act of 2020 (U.S. Senate, 2020b), and the Ethical Use of Facial Recognition Act (U.S. Senate, 2020a). The Facial Recognition and Biometric Technology Moratorium Act, for example, would prohibit federal use of face recognition and other biometric technologies and the use of federal funds for biometric surveillance (U.S. Senate, 2020b).

[4] State and local governments have regulated government use of certain technologies, including face recognition (e.g., California; Illinois; Somerville, Massachusetts). There are currently bans on official use of FRT in Boston; San Francisco; Oakland, California; Berkeley; Portland, Oregon; and Somerville, Massachusetts. Portland has also limited private business use, with an exception for the airport. In addition, several states (e.g., Illinois, California) have privacy laws that apply to biometric data. In total, more than a dozen cities or states have banned or restricted face recognition. See Harwell, 2021.

[5] In other cases, some technology companies have preferred to develop single sets of tools that comply with the most-restrictive applicable laws. Under this approach, a company would, for instance, apply more-restrictive privacy rules from one state, such as California, to other states rather than proceed under a checkerboard approach in which the company would have to design different tools to comply with the rules of different legal jurisdictions. For instance, see Brill, 2019.

[6] For instance, the National Institute of Standards and Technology plays a key role in testing face-recognition systems. See National Institute of Standards and Technology, 2020.

[7] See experts quoted in Gold, 2021.

[8] Hundreds of cognitive and affective biases exist. For further discussion, see Västfjäll and Slovic, 2013.

References

ACLU—*See* American Civil Liberties Union.

Ahlers, Mike M., "TSA Removes Body Scanners Criticized as Too Revealing," CNN, May 30, 2013. As of April 28, 2021: https://www.cnn.com/2013/05/29/travel/tsa-backscatter

Amazon, "We Are Implementing a One-Year Moratorium on Police Use of Rekognition," news release, June 10, 2020. As of June 19, 2021: https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition

American Civil Liberties Union, "Letter from Nationwide Coalition to Amazon CEO Jeff Bezos Regarding Rekognition," June 18, 2018. As of June 19, 2021: https://www.aclu.org/letter-nationwide-coalition-amazon-ceo-jeff-bezos-regarding-rekognition

———, "Coalition Letter Calling for a Federal Moratorium on Face Recognition," letter to the chair and the ranking member of the U.S. House of Representatives Committee on Oversight and Reform, June 3, 2019. As of June 19, 2021: https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition

Andrews, Travis M., "Why Dangerous Conspiracy Theories About the Virus Spread So Fast—and How They Can Be Stopped," *Washington Post*, May 1, 2020.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information," Washington, D.C.: Pew Research Center, November 15, 2019. As of April 28, 2021: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Baird, John C., and Elliot Jason Noma, *Fundamentals of Scaling and Psychophysics*, New York: Wiley, 1978.

Berger, Jonah, and Katherine L. Milkman, "What Makes Online Content Go Viral?" *Journal of Marketing Research*, Vol. 49, No. 2, April 2012.

Biden, Joseph R., "Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," Washington, D.C.: White House, Executive Order 13985, January 20, 2021. As of May 13, 2021: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/

Bleicher, Ariel, "Demystifying the Black Box That Is AI," *Scientific American*, August 9, 2017. As of May 26, 2021: https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/

Brill, Julie, "Microsoft Will Honor California's New Privacy Rights Throughout the United States," blog post, *Microsoft on the Issues*, November 11, 2019. As of June 19, 2021: https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/

Bruine de Bruin, Wändi, and Ann Bostrom, "Assessing What to Address in Science Communication," *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 110, Supp. 3, August 20, 2013, pp. 14062–14068.

Buolamwini, Joy, and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research: Conference on Fairness, Accountability and Transparency*, Vol. 81, 2018, pp. 77–91. As of June 19, 2021: http://proceedings.mlr.press/v81/buolamwini18a.html

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

Committee on Oversight and Reform, U.S. House of Representatives, "Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties," hearing, Washington, D.C., May 22, 2019. As of May 17, 2021: https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and

Dave, Paresh, "Google Faces Employee Petition to End Tech Sales to Police," Reuters, June 22, 2020. As of June 19, 2021: https://www.reuters.com/article/us-minneapolis-protests-google/google-faces-employee-petition-to-end-tech-sales-to-police-idUSKBN23T3B3

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

Dyer, Joel, and Blas Kolic, "Public Risk Perception and Emotion on Twitter During the Covid-19 Pandemic," *Applied Network Science*, Vol. 5, No. 1, 2020, art. 99. As of June 19, 2021: https://appliednetsci.springeropen.com/articles/10.1007/s41109-020-00334-7

Edelman, *Edelman Trust Barometer 2021*, ca. 2021. As of May 17, 2021: https://www.edelman.com/trust/2021-trust-barometer

Electronic Privacy Information Center, "EPIC v. DHS (Suspension of Body Scanner Program)," undated. As of April 28, 2021: https://epic.org/privacy/litigation/apa/tsa/bodyscanner/

European Commission, "Proposal for a Regulation of the European Parliament Laying Down Harmonised Rules on Artificial Intelligence," COM/2021/206 final, June 10, 2021. As of June 21, 2021: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence

Funk, Cary, "Key Findings About Americans' Confidence in Science and Their Views on Scientists' Role in Society," Washington, D.C.: Pew Research Center, February 12, 2020. As of April 28, 2021: https://www.pewresearch.org/fact-tank/2020/02/12/key-findings-about-americans-confidence-in-science-and-their-views-on-scientists-role-in-society/

Funk, Cary, and Brian Kennedy, "Public Confidence in Scientists Has Remained Stable for Decades," Washington, D.C.: Pew Research Center, August 27, 2020. As of April 28, 2021: https://www.pewresearch.org/fact-tank/2020/08/27/public-confidence-in-scientists-has-remained-stable-for-decades/

Gold, Ashley, "The Global Race to Regulate AI," *Axios*, April 22, 2021. As of May 17, 2021: https://www.axios.com/regulate-ai-artificial-intelligence-9afe3bd9-65c1-434a-a9de-59019ff8fd9b.html

Greene, Jay, "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM," *Washington Post*, June 11, 2020.

Halchin, L. Elaine, *Overview of the Federal Procurement Process and Resources*, Washington, D.C.: Congressional Research Service, RS22536, updated January 12, 2021. As of June 19, 2021: https://crsreports.congress.gov/product/details?prodcode=RS22536

Hammarlund, Rebecca, Kathleen Crapanzano, Jessica McGovern, Thanh Le, Sen Xu, Jennifer Reinovsky, and Maloa Affuembey, "Shooter Mental Illness Status and Language Use in Online Articles About Mass Shootings," *Stigma and Health*, Vol. 5, No. 2, 2020, pp. 225–229.

Harwell, Drew, "Civil Rights Groups Ask Biden Administration to Oppose Facial Recognition," *Washington Post*, February 17, 2021.

Haselton, Martie G., Daniel Nettle, and Paul W. Andrews, “The Evolution of Cognitive Bias,” in David M. Buss, ed., *The Handbook of Evolutionary Psychology*, Newark, N.J.: John Wiley and Sons, 2015, pp. 724–726.

Hill, Kashmir, “Wrongfully Accused by an Algorithm,” *New York Times*, June 24, 2020, updated August 3, 2020.

———, “Clearview AI’s Facial Recognition App Called Illegal in Canada,” *New York Times*, February 3, 2021a.

———, “Your Face Is Not Your Own,” *New York Times*, March 18, 2021b.

IBM, “IBM CEO’s Letter to Congress on Racial Justice Reform,” blog post, *THINKPolicy Blog*, June 8, 2020. As of June 19, 2021:
https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/

Illinois Compiled Statutes, Rights and Remedies; Chapter 740, Civil Liabilities; Section 14, Biometric Information Privacy Act. As of June 19, 2021:
https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

JAMRS—*See* Joint Advertising, Market Research and Studies.

Johnson, Dominic D. P., and James H. Fowler, “The Evolution of Overconfidence,” *Nature*, Vol. 477, 2011, pp. 317–320.

Joint Advertising, Market Research and Studies, homepage, undated. As of May 17, 2021:
https://jamrs.defense.gov/

Jones, Jeffrey M., “Democratic, Republican Confidence in Science Diverges,” Gallup, July 16, 2021. As of July 28, 2021:
https://news.gallup.com/poll/352397/democratic-republican-confidence-science-diverges.aspx

Kahneman, Daniel, and Shane Frederick, “Representativeness Revisited: Attribute Substitution in Intuitive Judgment,” in T. Gilovich, D. Griffin, and Daniel Kahneman, eds., *Heuristics and Biases: The Psychology of Intuitive Judgment*, Cambridge University Press, 2002, pp. 42–81.

Kasperson, Roger E., Ortwin Renn, Paul Slovic, Halina S. Brown, Jacque Emel, Robert Goble, Jeanne X. Kasperson, and Samuel Ratick, “The Social Amplification of Risk: A Conceptual Framework,” *Risk Analysis*, Vol. 8, No. 2, June 1988, pp. 177–187.

Kavanagh, Jennifer, and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, Calif.: RAND Corporation, RR-2314-RC, 2018. As of June 19, 2021:
https://www.rand.org/pubs/research_reports/RR2314.html

Lyons, Kim, “ICE Just Signed a Contract with Facial Recognition Company Clearview AI,” *The Verge*, August 14, 2020. As of June 19, 2021:
https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration

Macmillan, Neil A., and C. Douglas Creelman, *Detection Theory: A User’s Guide*, 2nd ed., Mahwah, N.J.: Taylor and Francis, 2004.

McCarney, Rob, James Warner, Steve Iliffe, Robbert van Haselen, Mark Griffin, and Peter Fisher, “The Hawthorne Effect: A Randomised, Controlled Trial,” *BMC Medical Research Methodology*, Vol. 7, 2007, art. 30. As of June 19, 2021:
https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/1471-2288-7-30

Morgan, M. Granger, Baruch Fischhoff, Ann Bostrom, and Cynthia J. Atman, *Risk Communication: A Mental Models Approach*, New York: Cambridge University Press, 2002.

Nakashima, Ellen, "DHS to Advise Telecom Firms on Preventing 5G Cell Tower Attacks Linked to Coronavirus Conspiracy Theories," *Washington Post*, May 13, 2020.

National Institute of Standards and Technology, U.S. Department of Commerce, "Face Recognition Vendor Test," created July 8, 2010, updated November 30, 2020. As of May 17, 2021:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Osoba, Osonde A., Benjamin Boudreaux, Jessica Saunders, J. Luke Irwin, Pam A. Mueller, and Samantha Cherney, *Algorithmic Equity: A Framework for Social Applications*, Santa Monica, Calif.: RAND Corporation, RR-2708-RC, 2019. As of June 19, 2021:
https://www.rand.org/pubs/research_reports/RR2708.html

Osoba, Osonde A., and William Welser IV, *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017. As of May 24, 2021:
https://www.rand.org/pubs/research_reports/RR1744.html

Ovide, Shira, "A Case for Banning Facial Recognition," *New York Times*, June 9, 2020, updated January 31, 2021.

Pennebaker, James W., Roger J. Booth, and Martha E. Francis, *Linguistic Inquiry and Word Count: LIWC2007—Operator's Manual*, Austin, Tex.: LIWC.net, undated. As of June 19, 2021:
http://www.gruberpeplab.com/teaching/psych231_fall2013/documents/231_Pennebaker2007.pdf

Pew Research Center, "Social Media Join the Anti-TSA Movement," Washington, D.C., December 2, 2010.

———, "Americans, Politics and Science Issues," Washington, D.C., July 1, 2015. As of May 13, 2021:
https://www.pewresearch.org/science/2015/07/01/americans-politics-and-science-issues/

Public Law 104-13, Paperwork Reduction Act of 1995, May 22, 1995. As of June 19, 2021:
https://www.govinfo.gov/app/details/PLAW-104publ13

Public Law 107-296, Homeland Security Act of 2002, November 25, 2002. As of May 12, 2019:
https://www.govinfo.gov/app/details/PLAW-107publ296

Rainie, Lee, Scott Keeter, and Andrew Perrin, "Trust and Distrust in America," Washington, D.C.: Pew Research Center, July 22, 2019. As of April 28, 2021:
https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america/

Richardson, Rashida, ed., *Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force*, AI Now Institute, New York University, December 2019. As of June 21, 2021:
https://ainowinstitute.org/reports.html

Slovic, Paul, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor, "The Affect Heuristic," *European Journal of Operational Research*, Vol. 177, No. 3, March 16, 2007, pp. 1333–1352.

———, "Risk as Analysis and Risk as Feelings: Some Thoughts About Affect, Reason, Risk and Rationality," in Paul Slovic, ed., *The Feeling of Risk: New Perspectives on Risk Perception*, Routledge, 2013, pp. 49–64.

Smith, Rick, "The Future of Face Matching at Axon and AI Ethics Board Report," Axon, June 27, 2019. As of May 17, 2021:
https://www.axon.com/news/ai-ethics-board-report

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

Stephens-Davidowitz, Seth, "How Googling Unmasks Child Abuse," *New York Times*, July 13, 2013.

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

Tellis, Gerard J., Deborah J. MacInnis, Seshadri Tirunillai, and Yanwei Zhang, “What Drives Virality (Sharing) of Online Digital Content? The Critical Role of Information, Emotion, and Brand Prominence,” *Journal of Marketing*, Vol. 83, No. 4, July 2019, pp. 1–20.

Tversky, Amos, and Daniel Kahneman, “Judgment Under Uncertainty: Heuristics and Biases,” *Science*, Vol. 185, No. 4157, September 27, 1974, pp. 1124–1131.

Tyson, Alec, and Brian Kennedy, “Two-Thirds of Americans Think Government Should Do More on Climate,” Washington, D.C.: Pew Research Center, June 23, 2020. As of April 28, 2021:
https://www.pewresearch.org/science/2020/06/23/two-thirds-of-americans-think-government-should-do-more-on-climate/

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. As of March 20, 2021:
https://uscode.house.gov/view.xhtml?req=(title:6%20section:185%20edition:prelim)

U.S. Customs and Border Protection, U.S. Department of Homeland Security, *CBP Trade and Travel Report: Fiscal Year 2020*, Washington, D.C., February 4, 2021. As of June 19, 2021:
https://www.cbp.gov/document/annual-report/cbp-trade-and-travel-fiscal-year-2020-report

U.S. Department of Homeland Security, *Department of Homeland Security Acquisition Manual*, Washington, D.C., October 2009. As of June 20, 2021:
https://www.hsdl.org/?abstract&did=31748

———, *Privacy Impact Assessment Update for the Automated Targeting System*, Washington, D.C., DHS/CBP/PIA-006(e), January 13, 2017. As of May 24, 2021:
https://www.dhs.gov/publication/automated-targeting-system-ats-update

———, “Core Values,” last published July 3, 2019a. As of May 17, 2021:
https://www.dhs.gov/core-values

———, “Mission,” last published July 3, 2019b. As of June 19, 2021:
https://www.dhs.gov/mission

———, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services*, Washington, D.C., DHS/ICE/PIA-054, May 13, 2020. As of May 24, 2021:
https://www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services

———, “Automated License Plate Reader (ALPR) Fact Sheet,” January 5, 2021. As of May 24, 2021:
https://www.dhs.gov/publication/st-automated-license-plate-reader-fact-sheet

U.S. House of Representatives, George Floyd Justice in Policing Act of 2020, H.R.7120, 116th Congress, placed on Senate legislative calendar July 20, 2020. As of June 19, 2021:
https://www.congress.gov/bill/116th-congress/house-bill/7120

U.S. Senate, Ethical Use of Facial Recognition Act, S.3284, 116th Congress, referred to the Committee on Homeland Security and Governmental Affairs February 12, 2020a. As of June 19, 2021:
https://www.congress.gov/bill/116th-congress/senate-bill/3284

———, Facial Recognition and Biometric Technology Moratorium Act of 2020, S.4084, 116th Congress, referred to the Committee on the Judiciary June 25, 2020b. As of May 17, 2021:
https://www.congress.gov/bill/116th-congress/senate-bill/4084

Västfjäll, Daniel, and Paul Slovic, "Cognition and Emotion in Judgment and Decision Making," in M. D. Robinson, E. Watkins, and E. Harmon-Jones, eds., *Handbook of Cognition and Emotion*, Guilford Press, 2013, pp. 252–271.

Vincent, James, "Amazon Employees Protest Sale of Facial Recognition Software to Police," *The Verge*, June 22, 2018. As of June 19, 2021:
https://www.theverge.com/2018/6/22/17492106/amazon-ice-facial-recognition-internal-letter-protest

Waldron, Lucas, and Brenda Medina, "When Transgender Travelers Walk into Scanners, Invasive Searches Sometimes Wait on the Other Side," ProPublica, August 26, 2019. As of April 28, 2021:
https://www.propublica.org/article/tsa-transgender-travelers-scanners-invasive-searches-often-wait-on-the-other-side

West, Darrell M., and John R. Allen, "How Artificial Intelligence Is Transforming the World," Washington, D.C.: Brookings Institution, April 24, 2018. As of May 26, 2021:
https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/

Wild, Susan, Emanuel Cleaver II, Yvette D. Clarke, Eliot L. Engel, Anna G. Eshoo, Jan Schakowsky, Adam Smith, Bobby L. Rush, Raúl M. Grijalva, Donald S. Beyer Jr., Gwen Moore, Marc Veasey, Joaquin Castro, Eleanor Holmes Norton, Alexandria Ocasio-Cortez, Ayanna Pressley, Rashida Tlaib, Alcee L. Hastings, Jimmy Gomez, Ro Khanna, Ilhan Omar, Mark Takano, and Adriano Espaillat, members, U.S. Congress, letter to acting Secretary of Homeland Security Kevin McAleenan about the Biometric Exit Program, June 13, 2019. As of May 17, 2021:
https://wild.house.gov/media/press-releases/reps-wild-cleaver-clarke-sound-alarm-over-cbp-s-unprecedented-use-facial

Yeung, Douglas, Rebecca Balebako, Carlos Ignacio Gutierrez Gaviria, and Michael Chaykowsky, *Face Recognition Technologies: Designing Systems That Protect Privacy and Prevent Bias*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-4226-RC, 2020. As of May 20, 2021:
https://www.rand.org/pubs/research_reports/RR4226.html

Yeung, Douglas, Sara Beth Elson, Parisa Roshan, S. R. Bohandy, and Alireza Nader, *Can Social Media Help Analyze Public Opinion? A Case Study of Iranian Public Opinion After the 2009 Election*, Santa Monica, Calif.: RAND Corporation, RB-9685-RC, 2012. As of June 19, 2021:
https://www.rand.org/pubs/research_briefs/RB9685.html

Yeung, Douglas, Inez Khan, Nidhi Kalra, and Osonde A. Osoba, *Identifying Systemic Bias in the Acquisition of Machine Learning Decision Aids for Law Enforcement Applications*, Santa Monica, Calif.: RAND Corporation, PE-A862-1, 2021. As of April 22, 2021:
https://www.rand.org/pubs/perspectives/PEA862-1.html

Acknowledgments

We are grateful to our reviewers, Melissa L. Finucane and Andrew J. Lohn, for their valuable comments on this Perspective. We would also like to thank Kelly Klima for significantly helping to bring the Perspective to fruition. Victoria Greenfield also provided us valuable input, and Lisa Bernard provided us excellent edits. Kathleen Deloughery in our sponsor's office also provided us fantastic feedback and direction. We also want to thank Keller Scholl for helpful conversations on this topic.

About This Perspective

The U.S. Department of Homeland Security (DHS) has sought to leverage emerging technologies, such as face recognition and risk-assessment algorithms, for a variety of domestic security and other purposes. These technologies are believed to offer increased accuracy, convenience, and speed to support DHS objectives. However, important stakeholders have raised concerns about these technologies, including concerns about inequity and privacy, and have sought to regulate the government's use of them and to galvanize opposition. The American public's views about the relative benefits and risks of DHS use of these rapidly emerging technologies are not well understood.

In this Perspective, we argue that it is crucial for DHS to better understand public perceptions of emerging technologies, and we identify several methods that might be used to attain such understanding. Richer comprehension of the public's views will help DHS ensure that it will use technologies in ways that the public supports and will help it be prepared for potential regulation, secure funding for technology programs, strengthen partnerships, and improve its strategic communications. This Perspective should be of interest to officials across the DHS enterprise, including those responsible for the acquisition, development, and implementation of new technologies; strategic communications; partnership development; and legislative engagement.

This research was sponsored by the DHS Science and Technology Directorate and conducted within the Acquisition and Development Program of the Homeland Security Operational Analysis Center (HSOAC) federally funded research and development center (FFRDC).

About the Authors

Benjamin Boudreaux. Ben Boudreaux (he/him) is a professor at the Pardee RAND Graduate School and a policy researcher at RAND working in the intersection of ethics, emerging technology, and human security. His current research focuses on the ethics of artificial intelligence (AI) (including on algorithmic fairness, biometric surveillance, and military AI applications) and on cyberspace policy. He has a Ph.D. in philosophy.

Douglas Yeung. Douglas Yeung is a social psychologist at the RAND Corporation and a member of the Pardee RAND Graduate School faculty. His recent work has explored how policymakers can use insight from emerging technologies (e.g., social media, mobile devices) for well-being and civic policymaking. He has a Ph.D. in psychology.

Rachel Steratore. Rachel Dryden Steratore is an associate policy researcher with core competencies in risk perceptions, communication, decisionmaking, and behavior. She uses a diverse set of methods to perform analyses and develop recommendations on risk-related topics, including mental-model interviews and surveys of diverse stakeholder groups, expert elicitations, and qualitative data analyses. She has a Ph.D. in engineering and public policy.

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

An FFRDC operated by the
RAND Corporation under
contract with DHS

The Homeland Security Act of 2002 (Section 305 of Public Law 107-296, 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 the Homeland Security Operational Analysis Center (HSOAC) as an FFRDC for the U.S. Department of Homeland Security (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.

The research presented in this Perspective does not necessarily reflect official DHS opinion or policy.

For more information on HSOAC, see www.rand.org/hsoac. For more information on this publication, visit www.rand.org/t/PEA691-1.

PE-A691-1