NOT READY FOR TAKEOFF

FACE SCANS AT AIRPORT DEPARTURE GATES

GEORGETOWN LAW
Center on Privacy & Technology

www.airportfacescans.com

DECEMBER 21, 2017

NOT READY FOR TAKEOFF

FACE SCANS AT AIRPORT DEPARTURE GATES

GEORGETOWN LAW
Center on Privacy & Technology

Harrison Rudolph, *Associate*
Laura M. Moy, *Deputy Director*
Alvaro M. Bedoya, *Executive Director*

RESEARCH

Clare Garvie, *Associate*
Sabrina McCubbin, *Chief Research Assistant*
Laura Ashley Harris, *Research Assistant*
Megan Iorio, *Research Assistant*
Nur Lalji, *Research Assistant*
Caroline Zitin, *Research Assistant*

DESIGN

Rootid

www.airportfacescans.com

DECEMBER 21, 2017

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

At Boston's Logan International Airport, travelers at one international boarding gate will be surprised that they are being told to stop before what looks like a sophisticated camera.[1] But it's more than just a camera—the device compares each traveler's face to a Department of Homeland Security (DHS) biometric database to verify her identity and flags as many as 1 in 25 travelers for further scrutiny. These face scans have been deployed at eight other airports, too.[2]

In Atlanta, Chicago, Las Vegas, Miami, New York City, Houston, and Washington, D.C., travelers departing on certain international flights have their faces scanned by DHS. If DHS' current plans are executed, every traveler flying overseas, American and foreign national alike, will soon be subject to a face recognition scan as part of this "biometric exit" program (see Sidebar 1).

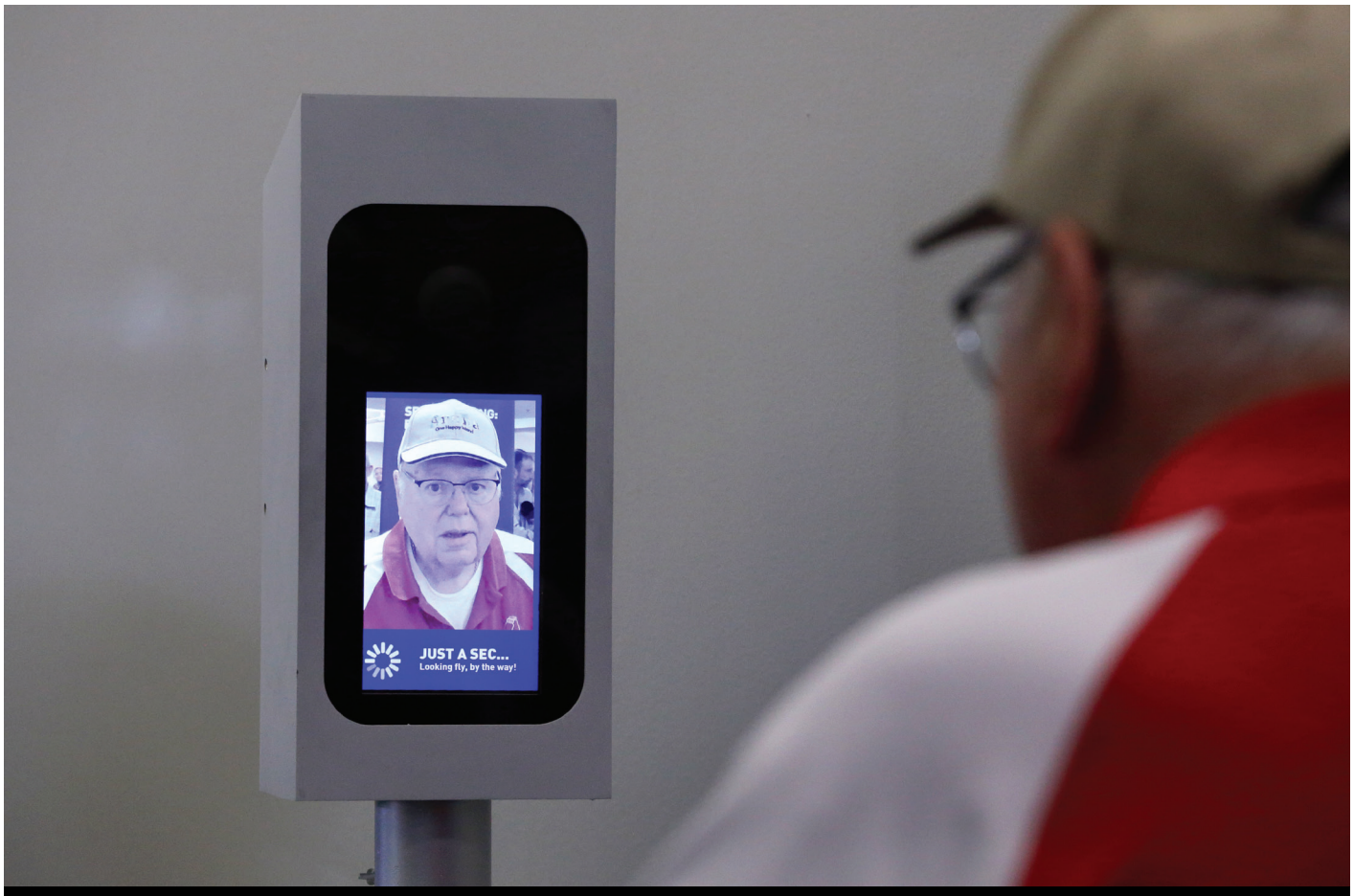


Figure 1: A man waits as his face is scanned at Logan Airport in Boston prior to boarding a flight to Aruba. (Photo: *Boston Globe*, all rights reserved)

This sophisticated biometric screening system could cost up to one billion dollars.[7] Congress has already created a "9-11 Response and Biometric Exit Account" to fund a biometric exit program in that amount.[8] Yet, curiously, neither Congress nor DHS has ever justified the need for the program. Congress never provided a rationale for it. For its part, DHS says that airport face scans are designed to verify the identities of travelers as they leave the country and stop impostors traveling under someone else's identity. But DHS itself has repeatedly questioned "the additional value biometric air exit would provide" compared with the status quo and the "overall value and cost of a biometric air exit capability," even as it has worked to build it.[9]

DHS should not be scanning the faces of Americans as they depart on international flights—but DHS is doing it anyway.

DHS' biometric exit program also stands on shaky legal ground. Congress has repeatedly ordered the collection of biometrics from foreign nationals at the border, but has never clearly authorized the border collection of biometrics from American citizens using face recognition technology.[10] Without explicit authorization, DHS should not be scanning the faces of Americans as they depart on international flights—but DHS is doing it anyway.[11] DHS also is failing to comply with a federal law requiring it to conduct a rulemaking process to implement the airport face scanning program—a process that DHS has not even started.[12]

Making matters worse, the face scanning technology used by DHS may make frequent mistakes. According to DHS' own data, DHS' face recognition systems erroneously reject as many as 1 in 25 travelers *using valid credentials*.[13] At this high rate, DHS' error-prone face scanning system could cause 1,632 passengers to be wrongfully delayed or denied boarding every day at New York's John F. Kennedy (JFK) International Airport alone.[14] What's more, DHS does not appear to have any sense of how effective its system will be at actually catching impostors—the system's primary goal.[15]

The privacy concerns implicated by biometric exit are at least as troubling as the system's legal and technical problems. As currently envisioned, the program represents a serious escalation of biometric scanning of Americans, and there are no codified rules that constrain it.[16] It may also lead to an even greater and more privacy-invasive government surveillance system. In addition, the program may hasten the development and deployment of privacy-invasive commercial technology by the airlines and technology vendors participating in biometric exit.

For now, DHS is moving forward with this expensive program. But Americans should consider whether it would be wiser to abandon DHS' airport face scan program and invest those funds elsewhere. If the program is to proceed, however, then at a minimum:

- DHS should justify its investment in face scans by supplying evidence of the problem it purportedly solves.
- DHS should stop scanning travelers' faces until it has completed a federally required rulemaking proceeding.

- DHS should stop scanning the faces of American citizens as they leave the country.
- DHS should prove that airport face scans are capable of identifying impostors without inconveniencing everyone else.
- DHS should adopt a public policy that prohibits secondary uses of the data collected by its airport face scan program.
- DHS should provide fairness and privacy guarantees to the airlines with which it partners.

In addition, in service to their customers, airlines should not partner with DHS in the future to conduct biometric screening of their passengers without first ensuring that DHS does all of the above, and without obtaining transparent and enforceable privacy, accuracy, and anti-bias guarantees from DHS.

Figure 2: A traveler has his face scanned as a Customs and Border Protection agent provides instruction. (Photo: Associated Press, all rights reserved)

SIDEBAR 1:
WHAT IS BIOMETRIC EXIT?

"Biometric exit" is a program that DHS operates that uses biometric data—data about a person's body—to verify travelers' identities as they leave the country. DHS initially tried to use fingerprint-based verification systems. These, however, disrupted traveler flow through airport terminals and were time-consuming and labor-intensive for administering personnel.[3] Under the latest iteration of the program, DHS has turned to face recognition.

Prior to departure of an outbound international flight, DHS prepopulates its "Traveler Verification Service" (TVS) with biometric templates of all travelers expected on the flight.[4] Upon reaching the airport gate to board the plane, each traveler is then asked to stand for a photo in front of a camera. The camera transmits the traveler's in-person photo to TVS, which compares it against the biometric templates on file. TVS then either confirms that the traveler's face matches the on-file biometric template(s) for an expected traveler—and creates a "biometrically verified exit record" for her—or rejects the traveler's face as a "non-match."[5]

If the traveler is rejected by the system, her credentials will be checked manually by a Customs and Border Protection (CBP) agent, or she will be subjected to another biometric check, such as a fingerprint comparison.[6]

II. FINDINGS

A. BIOMETRIC EXIT IS A SOLUTION IN SEARCH OF A PROBLEM

A review of the biometric exit program's history reveals that Congress never provided a rationale for it. DHS now claims the program is designed to detect a particular type of fraud defined in this report as "visa overstay travel fraud" (see Sidebar 2).[17] But available data on visa overstay travel fraud does not suggest that the problem is great enough to necessitate a massive and resource-intensive solution such as biometric exit.

The 9/11 Commission first recommended the adoption of a "biometrics-based entry-exit system" at the nation's borders in 2004.[18] Congress heeded the commission's call and, soon after, ordered DHS to "include a requirement for the collection of biometric exit data" from foreign nationals at the border.[19] Both the 9/11 Commission and Congress were clear that biometrics should be collected from foreign nationals *entering* the country to help detect criminals and terrorists before they set foot on American soil.[20] Neither, however, ever explained why it was necessary to collect biometrics from foreign nationals *leaving* the country.

DHS, for its part, has never studied whether there is a problem that necessitates a change in its approach to tracking travelers' departures. DHS claims that the aim of the program is to detect visa overstay travel fraud and to improve DHS' data on the departure of foreign nationals by "biometrically verifying" the exit records it already creates for those leaving the country.[21]

Visa overstay travel fraud could—in theory—be a problem worth solving. Foreign nationals who wish to remain in the country undetected past the expiration of their visas could be arranging to have others leave the country in their place using fraudulent credentials. But DHS has only ever published limited and anecdotal evidence of this. For example, one Immigration and Customs Enforcement (ICE) agent reportedly stated that the brother of a foreign national had traveled under his identity to generate a false exit record.[22]

Because the rationale for a biometric exit program is unclear, DHS has repeatedly expressed fundamental reservations about biometric exit. In 2012, DHS' Science and Technology (S&T) Directorate conducted an internal analysis of past failed fingerprint-based programs and came away skeptical of the very idea of biometric tracking at the border. S&T concluded that "significant questions remained" concerning "the additional value biometric air exit would provide" compared with the status quo and the "overall value and cost of a biometric air exit capability."[23] Four years later, in January 2016, DHS told the Government Accountability Office that it was still developing a report—and could not estimate when it would be completed—answering these two basic, fundamental questions.[24] As of publication of this paper, DHS had yet to release any such report.

SIDEBAR 2:

WHAT IS VISA OVERSTAY TRAVEL FRAUD?

"Visa overstay travel fraud" refers to a situation in which a foreign national wishes to remain in the United States undetected past the expiration of his visa and, to do so, arranges to have a conspirator leave the country in his place using the visa holder's credentials. This creates an "exit record" in the visa holder's name, fraudulently leading the government to believe that the visa holder has left the country, when in fact he has remained past the expiration of the visa, or "overstayed."

For example, if John Doe were about to overstay his visa, he could ask a conspirator, John Roe, to leave the country using his passport. If successful, DHS' departure tracking system would believe Doe had left the country when, in reality, only Roe had left.

DHS describes an exit record generated after a face scan as a "biometrically verified exit record." A fraudulent biometrically verified exit record would be an exit record where an impostor's face was scanned and erroneously accepted at the boarding gate.

DHS' uncertainty about biometric exit extends to the current face scan-based program. At a DHS Data Privacy and Integrity Advisory Committee meeting in September 2017, a committee member asked how DHS' face scanning system would benefit the nation's immigration system. Instead of identifying these benefits, a senior DHS official paused, then responded tellingly: "It's not the role of the administrative agency to question what laws are passed. It's our job to implement laws that are duly passed by Congress."[25]

B. DHS' AIRPORT FACE SCAN PROGRAM MAY VIOLATE FEDERAL LAW

DHS' current face scan-based program also may not comply with federal law. The program may exceed the authority granted to DHS by Congress because Congress has never explicitly authorized biometric collections from Americans at the border.[26] Even if DHS has sufficient legal authority for the program, DHS has failed to complete a prerequisite public rulemaking process for the program, as mandated by federal law.

If Congress wanted to tell DHS to collect Americans' biometrics at the border, it easily could have done so. It never has.

Congress has passed legislation at least nine times concerning authorization for the collection of biometric data from foreign nationals, but no law directly authorizes DHS to collect the biometrics of *Americans* at the border.[27] Congress has authorized the collection of biometrics at the border from, variously, "every alien departing the United States,"[28] "all categories of individual who are required to provide biometric entry data,"[29] and "every alien participating in the visa waiver program,"[30] but U.S. citizens have been conspicuously absent from the statutory text of every law under this program for the last 14 years.[31] If Congress wanted to tell DHS to collect Americans' biometrics at the border, it easily could have done so. It never has. Without explicit authorization, DHS cannot and should not be scanning the faces of Americans as they depart on international flights, as it is currently doing.

Even if it had the necessary authorization from Congress, DHS' biometric exit program would still be legally problematic because DHS has failed to complete a rulemaking process, which the federal Administrative Procedure Act (APA) requires it to do.[32] In a "notice-and-comment rulemaking," an agency solicits and considers feedback from interested members of the public before adopting an important new policy. Rulemaking provides the public an opportunity to participate in agency policymaking, but it also serves to put the public on notice of what an agency is doing and why, and what rules apply to an agency's new policy. In July, the Trump administration ordered DHS to initiate a rulemaking for the program by October 2017.[33] But DHS has not even begun the required process, even though DHS has already scanned the faces of tens of thousands of travelers across nine American airports—more than 36,000 in Atlanta alone.[34]

This is not the first time DHS has deployed a new privacy-invasive tool without conducting a required rulemaking process. In fact, a few years ago, under similar circumstances, a federal

appeals court held that DHS was required to go through the rulemaking process before using body scanners at Transportation Security Administration (TSA) checkpoints.[35]

DHS must conduct a rulemaking because mandatory biometric screening, like the body scanners program, constitutes a policy with the force of law. As the court found in the body scanners case a few years ago, even though requiring a passenger to pass through an existing checkpoint "is hardly novel," the adoption of a new screening technology at the existing checkpoint may nevertheless amount to a substantive change necessitating a rulemaking when it raises substantial privacy interests.[36] As with body scanners, privacy advocates have expressed deep concerns about airport biometrics,[37] and DHS itself has repeatedly raised privacy interests as relevant to its face scanning systems.[38] DHS is apparently aware of its obligation to conduct a rulemaking on biometric exit; several years ago, it initiated a rulemaking for a now-defunct fingerprint-based biometric exit program.[39]

The fact that DHS' airport face scanning program is only in operation at nine airports so far does not relieve DHS of its obligation to conduct a rulemaking process. As the court found in the body scanners case, rulemaking requirements apply at the point in time when an agency's pronouncement is "of present binding effect."[40] In that case, even though body scanners were only in use in some airports, the court found that the scanners were nevertheless "binding" on passengers, because any individual passenger would still be "bound to comply with whatever screening procedure the TSA is using on the date he is to fly at the airport from which his flight departs."[41] Face scans at specific exit gates are similarly binding on the travelers who pass through those gates. Face scans are strictly mandatory for foreign nationals, and although DHS has said that face scans may be optional for some American citizens, it is unclear whether this is made known to American travelers.[42] A rulemaking is therefore overdue.

C. DHS' AIRPORT FACE SCAN PROGRAM MAY BE TECHNICALLY FLAWED

DHS' face scan-based biometric exit program may also fail as a technical matter: DHS has never measured the efficacy of airport face scans at catching impostors traveling with fraudulent credentials.[43] There is good reason to be skeptical of the system's efficacy. Due to the challenges inherent to face recognition, it would be difficult for DHS to develop a system that is effective at catching every impostor without severely inconveniencing all other travelers.

DHS appears to have no idea whether its system will be effective at achieving its primary technical objective.

Problematically, DHS uses the wrong metric to evaluate the system's success. DHS currently measures performance based on how often the system correctly accepts travelers who are using true credentials.[44] But if the aim of this system is to detect and stop visa overstay travel fraud—as DHS suggests—it is critical and perhaps *more* important to assess how well it performs at correctly rejecting travelers who are using fraudulent credentials. Yet DHS is not measuring that.[45]

SIDEBAR 3:

UNDERSTANDING FACE RECOGNITION MISTAKES

Face recognition technology is not perfect.[47] If it were, it would always correctly *accept*—and clear for boarding—each traveler using her own valid credentials (a "**True Accept**") and would always correctly *reject* any traveler using fraudulent credentials, e.g., someone else's identification documents (a "**True Reject**").

In reality, face recognition systems make mistakes on both of those fronts. In the case of a "**False Reject**," a system fails to match an airport photo of a traveler's face to the photo on the traveler's own valid identification documents. A system may mistakenly reject a traveler flying under his *own* identity, for example, because his photo on file was taken four years prior and he has changed appearance since then.

In contrast, in the case of a "**False Accept**," the system mistakenly matches an airport photo of a traveler's face to someone else's photo. For example, a face scanning system may mistakenly accept an impostor fraudulently presenting someone else's travel credentials as her own.

As an analogy, consider a bouncer hired to check IDs at a bar. The bar's owner may be annoyed at a bouncer who accidentally turns away customers using their real IDs. But the owner will almost certainly fire a bouncer who consistently allows entry to underage patrons using fake IDs. Like a bar owner who has not even asked how well a bouncer can identify fake IDs, DHS appears to have no idea whether its system will be effective at achieving its primary technical objective.

In fact, it may not be possible, given the current state of face recognition technology, to succeed on both of these fronts. There is an unavoidable trade-off between these two metrics: A system calibrated to reduce rejections of travelers using valid credentials will increase acceptance rates for impostors.[46] For biometric exit, DHS may therefore have to choose between a system that catches impostors at a high rate but also incorrectly rejects valid credentials at a high rate—shunting innocent travelers into additional screening and causing delays—and a system that rejects valid credentials at a much lower rate but also underperforms at catching impostors.

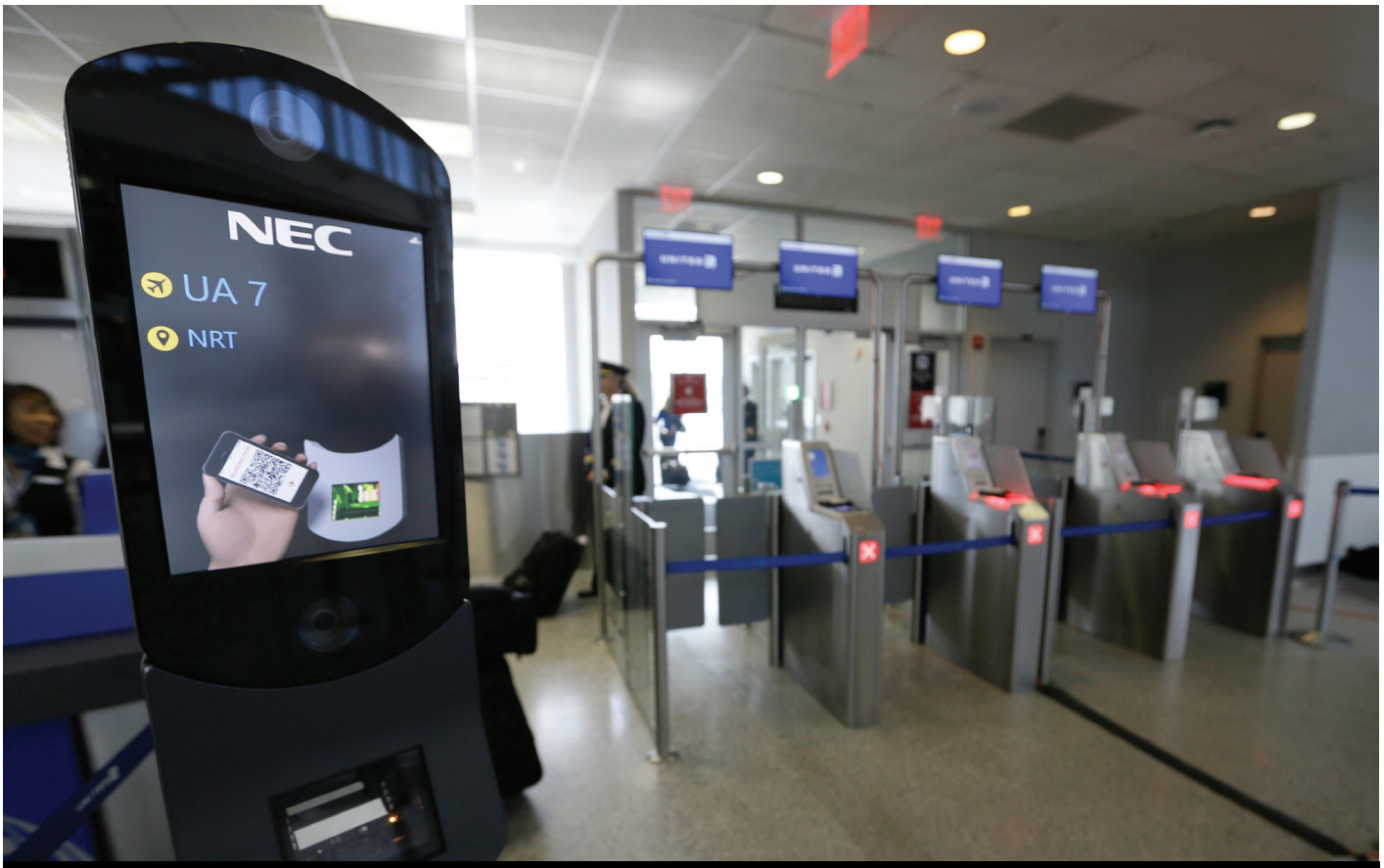


Figure 3: A face recognition device at a United Airlines gate at Houston's George Bush Intercontinental Airport. (Photo: Associated Press, all rights reserved)

DHS clearly is focusing on making its face scan system minimally inconvenient for travelers using valid credentials. DHS' sole accuracy requirement for the system is that 96 percent—or at least 24 out of 25—of travelers flying under their own identity are correctly accepted by the system and allowed to proceed to boarding.[48] But due to the trade-off explained above, emphasizing the success of the system at verifying valid credentials—perhaps to minimize unnecessary hassle and delays at already-busy international airports—may increase the risk that impostors go undetected.

Indeed, analysis of face recognition algorithms indicates that some likely comparable systems would not perform well at screening the type of impostor the system is likely to encounter: someone who fraudulently uses the boarding documents of a different person of the same age, gender, and country of origin or ethnicity. According to research conducted by the National Institute of Standards and Technology (NIST), face recognition systems, like humans, have a harder time distinguishing among people who look alike.[49] The algorithms tested by NIST are more likely to falsely match individuals who are similar in appearance, a fact that NIST notes "present[s] a security vulnerability to, for example, a passport gate."[50]

DHS has also acknowledged that it is unable to determine whether its airport face scans' accuracy varies depending on travelers' demographic characteristics—even though the latest research suggests that DHS' system may perform differently based on travelers' race and gender (see Sidebar 4). DHS indicated that it has been testing whether its face scanning system exhibits bias.[51] DHS even tasked the DHS Data Privacy and Integrity Advisory Committee with investigating solutions for such problems.[52]

But DHS has conceded that its internal testing remains inconclusive because of the limited sample size.[53] As a consequence, DHS may well be deploying a system that will exhibit race- or sex-biased decisions.

Innocent people may be pulled from the line at the boarding gate and subjected to manual fingerprinting at higher rates as a result of their complexion or gender.

Differential error rates could mean that innocent people will be pulled from the line at the boarding gate and subjected to manual fingerprinting at higher rates as a result of their complexion or gender. But because DHS has subsumed its evaluative process into a neutral-seeming computer algorithm, this bias may go undetected.

D. DHS' AIRPORT FACE SCAN PROGRAM RAISES BROADER CONCERNS ABOUT THE EXPANSION OF GOVERNMENT SURVEILLANCE

Following the January 2017 "Muslim Ban" executive order that would have banned people from seven Muslim-majority countries from entering the U.S., demonstrators spontaneously gathered at airports across the country to protest the policy.[59] What if the same technology currently used at departure gates were also used to identify protesters? What if it didn't just verify individuals' identities but also compared their faces to those of suspected criminals or terrorists?

SIDEBAR 4:
FACE RECOGNITION AND BIAS

Since February 2017, NIST has tested more than 35 different face recognition algorithms designed to verify identities.[54] Many of the algorithms tested exhibited different error rates depending on the race and gender of the person being scanned.

Most face scanning algorithms function by first calculating the approximate similarity of two images presented for comparison, then accepting the presented images if the similarity calculation is greater than a predetermined match threshold, and rejecting the presented images if the calculation falls below the threshold.[55] According to NIST's research, of the algorithms tested that use this method, most have been found more likely to mistakenly reject men, especially white men. At the same time, the tested algorithms were more likely to mistakenly accept women, especially black women.[56]

These results differ from earlier research suggesting that certain face recognition systems may more often fail to identify African-Americans and women,[57] but the two bodies of research share a common, and concerning, conclusion: Face recognition may perform differently as a result of variations in race or gender.[58] This is a possibility that DHS must test and address.

DHS' airport face scans raise important questions about the expansion of government tracking tools in public spaces. As currently envisioned, biometric exit is limited to certain areas of specific airports, but the program may be expanded to additional privacy-invasive applications and may be made interoperable with other law enforcement agencies' systems at the state, local, or federal level. The effects of these policies on free speech and association could be significant.

DHS intends to subject every single traveler who departs for an international destination—American and foreign national alike—to biometric exit. As the Privacy Impact Assessment for the program pointedly states, when traveling internationally, "the only way for an individual to ensure he or she is not subject to collection of biometric information . . . is to *refrain from traveling*."[60] American citizens make almost 50 million international journeys by air each year.[61] With the added millions of trips taken by foreign nationals departing from the U.S. each year, the total number of face scans annually will be even larger than that.[62]

Right now, scans generally take place at international departure gates and are conducted as travelers board the plane, arguably with the awareness of the scanned individual. But DHS is already exploring expansions to other areas of the airport. At New York's JFK Airport, travelers headed for international flights recently were asked to submit to a face scan by CBP personnel at a TSA checkpoint—not at their departure gate.[63] According to a DHS press release, "CBP is assessing the use of biometric technology as part of a future end-to-end process, from check-in to departure, in which travelers use biometrics instead of their boarding pass or ID throughout the security and boarding process."[64]

As DHS invests hundreds of millions of dollars into expanding its face scanning capability, airport face scans could even be extended to include passive scans throughout American airports—including of domestic travelers in domestic airports. One proposal in Congress—the TSA Modernization Act—would authorize TSA to use biometrics to identify and track travelers at any area "where such deployment would enhance security and facilitate passenger movement."[65] That could mean real-time face recognition surveillance cameras at "checkpoints, screening lanes, bag drop and boarding areas."[66]

The broader reaching and more constant face scans become, the more they will threaten to chill free speech and thwart free association in airports.

The technology could also be adapted for purposes unrelated to air travel, including general law enforcement and counterterrorism initiatives. For example, one high-profile bill in Congress, the Border Security for America Act, would require DHS to begin using airport face scans to find matches against the FBI's Terrorist Screening Database.[67] That expansion would incentivize DHS to make its system linkable to and interoperable with other FBI or state criminal law enforcement databases. Because face recognition technology makes mistakes, counterterrorism and law enforcement face scans could result in the investigation of innocent people for crimes they didn't commit. These errors may also vary on the basis of those individuals' race or gender.

Figure 4: Crowds gather at San Francisco International Airport to protest the "Muslim Ban" in January 2017. (Photo: Peg Hunter, CC BY-NC 2.0)

The broader reaching and more constant face scans become, the more they will threaten to chill free speech and thwart free association in airports. The perception of being under surveillance encourages people to censor what they say, especially when they hold minority or dissenting viewpoints.[68] Because airports are increasingly prominent sites of political speech, any ramp-up of biometric surveillance in these spaces—especially without data use restrictions—could severely impact free speech and association.[69]

E. DHS' AIRPORT FACE SCAN PROGRAM ALSO INCREASES PRIVATE ENTITIES' ACCESS TO SENSITIVE TRAVELER DATA

So far, this paper has focused on concerns arising from the government's operation of its biometric exit program. But this program also makes travelers vulnerable to increased and unconstrained tracking by private companies. That's because DHS relies heavily on airlines and technology vendors for central components of the airport face scan program, from provision

of software and hardware, to collection and transmission of data, to processing of passenger photos, and more. By relying on private entities, DHS facilitates the sharing of sensitive traveler information with outside companies that have their own business interests.[70] Yet, despite the risk that airlines will use biometric exit data and technology for their own tracking purposes,[71] DHS has not published any guidelines for or agreements with its private partners.[72]

At every step of the biometric exit process, private entities are heavily involved. For example, DHS is collaborating with JetBlue and air travel IT and communications vendor SITA to build and operate biometric exit for select JetBlue's flights.[73] Delta has been working with vendors Vision-Box and NEC.[74]

There are few protections to ensure that biometric exit data and technology will not be abused.

Some airlines may well begin to explore ways to further monetize the technology they develop, for example by enhancing targeted advertising capabilities in airports. Indeed, at a recent event in Menlo Park, California, an investment associate from JetBlue Technology Ventures indicated that the company's airline is interested in developing or using face scanning or other biometric technology to "hypertarget" customers for advertising purposes.[75]

Some, if not all, of what airlines and technology partners may do with any data or technology to which they gain access through participation in biometric exit may be constrained by agreements with DHS. For example, DHS has disclosed that it has reached a Memorandum of Understanding with JetBlue that encompasses JetBlue's handling of biometric exit data.[76] But as of publication of this paper, neither that Memorandum of Understanding nor any other agreement governing private entities' use of biometric exit data has been made public. Without greater transparency regarding such private agreements and without substantive rules governing the role of private entities in the biometric exit process, there are few protections to ensure that biometric exit data and technology will not be abused.

III. RECOMMENDATIONS

- **Recommendation 1: DHS should justify the face scan-based biometric exit program by identifying the problem it is attempting to solve, quantifying the scope of that problem, and explaining why this program is needed to solve it.**

As it currently stands, the biometric exit program is unjustified. If the program is indeed designed to address visa overstay travel fraud, then DHS should study how often this type of fraud likely occurs, publish the results, and demonstrate that it is a problem worth solving. This could be done using data already available to the agency. For example, DHS could review historical data concerning the incidence of visa overstays entering U.S. law enforcement or DHS custody despite the existence of a biographic exit record in DHS' existing repository containing data about the arrival and departure of travelers, the Arrival and Departure Information System (ADIS).[77] Such a study would lend much-needed insight into whether visa overstay travel fraud is common and thus into whether a billion-dollar solution to the problem is warranted.

- **Recommendation 2: DHS should suspend airport face scans pending completion of a federally required rulemaking proceeding.**

DHS should suspend all airport face scans at departure gates until it comes into compliance with federal administrative law. As detailed above, the law requires DHS to solicit and consider comments from the public before adopting big-impact new programs like mandatory biometric scans. DHS must issue a Notice of Proposed Rulemaking, respond to public comments, and issue a Final Rule putting the public on notice about airport face scans and the rules that apply to them.

- **Recommendation 3: DHS should stop scanning the faces of American citizens as they leave the country.**

DHS should exclude Americans from any biometric exit program. Congress has never explicitly authorized DHS to routinely scan the faces of U.S. citizens at airports. Unless and until it receives a congressional mandate to resume airport face scans of Americans, DHS should work to preserve and improve upon manual passport-face comparisons conducted at the TSA security checkpoint by TSA agents and at the boarding gate by gate agents.

- **Recommendation 4: DHS should demonstrate that its technology is sufficiently advanced to stop impostors without inconveniencing everyone else.**

DHS should study how well its face recognition technology works and publish the results. DHS should engage in an ongoing evaluation of both the effectiveness of its system at detecting impostors under operational conditions and the rate at which its system falsely rejects individuals who are presenting their own valid credentials. DHS should also evaluate its system's performance on a diverse population. Any result that indicates that the algorithm performs differently based on travelers' race or gender

would be unacceptable and must be corrected prior to deployment.

- **Recommendation 5: DHS should adopt a public policy that ensures data collected by any airport face scan program will not be used for other purposes.**

To protect traveler privacy, DHS should adopt public policies strictly limiting the use of data collected by face scanning systems to the purpose for which it is to be collected—to verify foreign national travelers' identities as they depart from the United States. The use restrictions applicable to data collected by any airport face scan program should include an explicit prohibition on sharing collected data with state, local, or federal law enforcement without a warrant or lawfully issued court order.

- **Recommendation 6: Airlines should condition partnerships with DHS on fairness and privacy guarantees.**

In service to their customers, airlines should not partner with DHS in the future to conduct biometric screening of travelers without first obtaining enforceable privacy, error rate, and guarantees against bias. The airlines should also demand that DHS adopt a policy that, as detailed above, limits the use of data collected by any airport face scanning program to the purpose for which it is collected. The airlines should ensure that all policies applicable to airport face scans are made publicly available and easily accessible to travelers. And airlines should require that any updates or revisions to these policies be accompanied by a public notification of the alteration. These requirements should be paired with commitments from DHS to study and remedy system bias and to enhance system accuracy rates.

It may fall to airline shareholders to inform the corporate boards of the risks of unmitigated airport biometric technologies. To that end, shareholders may wish to recommend via shareholder resolutions that the corporate boards adopt a policy prohibiting voluntary participation in Homeland Security biometric projects.

IV. CONCLUSION

The face scan-based biometric exit program that DHS is beginning to deploy at international airports across the country is extremely resource-intensive. But despite its $1 billion price tag, the program is riddled with problems. It is unjustified. It is legally infirm. It may be technically flawed. And it may implicate serious privacy concerns.

For all of the above reasons, Americans should consider whether perhaps it would be wiser to abandon DHS' face scan-based biometric exit program, which is costly but offers no tangible benefits and many concerns. If DHS persists with the program, significant reforms are vitally necessary.

V. ACKNOWLEDGEMENTS

The Electronic Privacy Information Center's important work litigating a case regarding the privacy implications of body scanners in airports—cited multiple times in this report—was in many ways foundational to this report, as were the oversight actions of the Government Accountability Office, and the reports and stakeholder meetings of the Department of Homeland Security. This report was also made possible by the research of Clare Garvie, the Center on Privacy & Technology's resident face recognition expert, and the vigilance and gentle guidance of Katie Evans, who handles both operations and communications for the Center.

Critical guidance and close reading were provided by Professors Paul Ohm and David Vladeck, both of whom are Center faculty directors. The remainder of our expert reviewers will remain anonymous, but we are deeply thankful for their time and attention to this effort. We would also like to thank the Center's research assistants, our copy editor, Joy Metcalf, our communications firm, Spitfire, and our design and web development firm, Rootid.

The Center on Privacy & Technology at Georgetown Law is supported by the Ford Foundation, the MacArthur Foundation, the Media Democracy Fund, the Omidyar Network, the Open Society Foundations, and the Georgetown University Law Center. We are particularly grateful for additional support from the MacArthur Foundation that allowed us to successfully complete this report.

VI. ABOUT THE AUTHORS

Harrison Rudolph is an associate at the Center on Privacy & Technology at Georgetown Law. Harrison received his B.A. from The George Washington University and his J.D. from Georgetown Law. Before law school, Harrison worked as a paralegal at a law firm focusing on issues impacting consumer credit reporting agencies.

Laura M. Moy is the deputy director of the Center on Privacy & Technology at Georgetown Law. Before joining the Center, Laura was acting director of the Communications & Technology Clinic at Georgetown Law's Institute for Public Representation. Prior to that, she worked at New America's Open Technology Institute and Public Knowledge. Laura completed her J.D. at New York University School of Law and her LL.M. at Georgetown.

Alvaro M. Bedoya is the founding executive director of the Center on Privacy & Technology at Georgetown Law and co-author of *The Perpetual Line-Up: Unregulated Police Face Recognition in America,* the Center's 2016 report. Previously, he was chief counsel to the Senate Judiciary Subcommittee on Privacy, Technology & the Law. He is a graduate of Harvard College and Yale Law School.

VII. ENDNOTES

1. *See Board in a Snap: JetBlue to Launch First-of-Its-Kind Self-Boarding Program Using Facial Recognition*, JetBlue (May 31, 2017), http://www.mediaroom.jetblue.com/investor-relations/press-releases/2017/05-31-2017-112155081.

2. *See CBP Deploys Biometric Exit Technology to Miami International Airport*, U.S. Customs and Border Protection (Oct. 20, 2017), https://www.cbp.gov/newsroom/local-media-release/cbp-deploys-biometric-exit-technology-miami-international-airport.

3. U.S. Government Accountability Office, GAO-13-683, Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program Report to Congressional Requesters 27–28 (July 2013), https://www.gao.gov/assets/660/656316.pdf.

4. To prepopulate TVS with biometric templates of expected travelers, DHS draws from photos captured by CBP during previous entry inspections, photos from U.S. passports and U.S. visas, and photographs from other DHS encounters, which "may include those from DHS apprehensions or enforcement actions, previous border crossings, and immigration records." U.S. Department of Homeland Security, DHS/CBP/PIA-030(c), Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process 4 (June 12, 2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-june2017.pdf (hereinafter "Traveler Verification Service (TVS): Partner Process"). Because accuracy is highly dependent on image quality, the inclusion of photos from sources other than passport and visa databases, such as law enforcement encounters, likely lowers overall system accuracy rates beyond what is assumed in this paper. *See* Patrick Grother & Mei Ngan, NIST Interagency Report 8009, Face Recognition Vendor Test (FRVT) Performance of Face Identification Algorithms, National Institute of Standards and Technology 26–27 (May 26, 2014), http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=915761 (demonstrating that comparing webcam images (a proxy for lower quality photos from other DHS encounters) against mugshot images (a proxy for the in-person traveler photo taken at the gate) yielded the lowest recognition accuracy rates due to the heterogeneity of image types and quality).

5. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4.

6. *See id.* at 2, 5. Rejected foreign travelers will be subjected to "manual officer exception processing." *Id.* Under the system's most recent prior iteration, manual officer processing involved a fingerprint query in the IDENT database, and where an officer "was unable to locate an IDENT fingerprint record" a "separate criminal history check in the Federal Bureau of Investigation's Next Generation Identification" database. *Id.*

7. Consolidated Appropriations Act, Pub. L. No. 113-114 § 411(c)(2)(B), 129 Stat. 2242, 3006 (2016), https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.

8. *Id.* § 411.

9. U.S. Government Accountability Office, GAO-16-358T, *Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System: Before the Subcommittee on Immigration and the Nat'l Interest, Committee on the Judiciary*, U.S. Senate, 115th Cong. 8 (Jan. 20, 2016) (Statement of Rebecca Gambler, Director Homeland Sec. and Justice), https://www.gao.gov/assets/680/674704.pdf.

10. *See infra* Section B.

11. Under federal law, it is unlawful for any DHS action to be "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right . . . ." 5 U.S.C. § 706 (2)(C).

12. *See* 5 U.S.C. § 553(b).

13. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4, at 13 ("CBP requires an accuracy goal of 96% TAR for facial images acquired in an airport/seaport exit environment"); *infra* Section C (defining True Accept rates).

14. According to the latest data available, taking the extra time to process rejected passengers could translate into more time spent on the tarmac for every traveler. When CBP deployed a fingerprint-based biometric solution, it took six CBP officers 45 minutes to collect fingerprints from 75 passengers. Government Accountability Office, GAO-17-170, Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain 15 (Feb. 2017), https://www.gao.gov/assets/690/683036.pdf. This is equivalent to approximately 3.6 minutes per passenger for each CBP agent. CBP has never suggested that more than one CBP officer or airline gate agent will fingerprint rejected travelers. At a reject rate of 1 in 25—DHS' own standard—a face scanning device screening the 335 travelers boarding a Dreamliner aircraft would reject approximately 14 passengers. If all of these rejected travelers are foreign nationals, then according to the GAO report, it would take 3.6 minutes to fingerprint each one. At that rate, assuming that false rejections occur at a regular interval (and are not back-loaded, which would delay boarding even further), CBP would need more than 50 minutes from the beginning of boarding just to screen rejected travelers. Separately, approximately 40,799 passengers depart on international flights from JFK each day. See Airport Traffic Report,

The Port Authority of New York and New Jersey 50 (Apr. 1, 2016), https://www.panynj.gov/airports/pdf-traffic/ATR_2015.pdf. If 1 in 25 of those travelers is falsely rejected—the highest acceptable error rate by DHS' own standard—that would mean approximately 1,632 passengers would be wrongfully denied boarding. At Boston Logan International Airport, 494,741 international travelers deplaned or boarded during the month of January 2017. See Monthly Airport Traffic Summary, Massport (Jan. 2017), http://www.massport.com/media/1962/0117-avstats-airport-traffic-summary.pdf. If half of those passengers were outbound departures, 247,371 passengers in January—or 7,980 passengers each day—departed from Boston Logan International Airport. At a rate of 1 in 25, that would mean 319 passengers would be wrongfully denied boarding at Logan Airport on a daily basis.

15. *See infra* Section C.

16. *See infra* Section D.

17. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4, ("[T]he TVS . . . confirm[s] the identity of the traveler, create[s] an exit record, and biometrically confirm[s] the exit of in-scope non-U.S. citizens."); U.S. Department of Homeland Security, DHS-2008-0039-0002, Air/Sea Biometric Exit Project: Regulatory Impact Analysis 67–68 (Apr. 17, 2008), *available at* https://airlineinfo.com/dhspdf/3.pdf; *see also* Ron Nixon, *Border Agents Test Facial Scans to Track Those Overstaying Visas*, New York Times (Aug. 1, 2017), https://www.nytimes.com/2017/08/01/us/politics/federal-border-agents-biometric-scanning-system-undocumented-immigrants.html ("The pilot effort is part of a decades-long push to more accurately identify people who overstay their visas and remain in the United States, a group that represents the largest number of people in the United States illegally . . . . Homeland Security officials say they believe the entry and exit biometric system can also be used to crack down on illegal immigration . . . . In the absence of a biometric entry and exit system, the agency depends on incomplete data from airline passenger manifests to track people who leave the country.").

18. National Commission on Terrorist Attacks upon the U.S., The 9/11 Commission Report 389 (July 22, 2004), *available at* https://www.9-11commission.gov/report/911Report.pdf (hereinafter "9/11 Commission Report") ("funding and completing a biometrics-based entry-exit system is an essential investment in our national security.").

19. Congress codified the Commission's recommendation by amending DHS' biographical system for tracking visa overstays at the border to require collection of biometric exit data "for all categories of individuals who are required to provide biometric entry data." Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208 (2004), https://legcounsel.house.gov/Comps/Intelligence%20Reform%20And%20Terrorism%20Prevention%20Act%20Of%202004.pdf. This includes foreign nationals except those who are under the age of 14, over the age of 79, and diplomats. *Id.*

20. *See* 9/11 Commission Report, *supra* note 18; Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208(a) (2004) ("Congress finds that completing a biometric entry and exit data system as expeditiously as possible is an essential investment in efforts to protect the United States by preventing the entry of terrorists.").

21. *See* Ron Nixon, *supra* note 17.

22. Office of Inspector General, OIG-17-56, DHS Tracking of Visa Overstays is Hindered by Insufficient Technology 21 (May 1, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-56-May17_0.pdf.

23. *See supra* note 9.

24. *Id.* at 10.

25. U.S. Department of Homeland Security Data Privacy and Integrity Advisory Committee (DPIAC) Meeting (Sept. 19, 2017) (notes on file with author); *see also* U.S. Department of Homeland Security, DPIAC Meeting Minutes 5 (Sept. 19, 2017), https://www.dhs.gov/sites/default/files/publications/DPIAC%20Meeting%20Minutes-Sept%2019%202017.pdf (alternatively noting the cited interaction as: "Q(LG): does this solve your problem with overstaying/terrorism? A(MH): not our role to question duly passed laws from Congress. We think it gives us immigration and counterterrorism benefits. We trust in Congress and 9/11 Commission.").

26. *See supra* note 11.

27. *See* Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546 (1996); Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106-215, 114 Stat. 337 (2000); Visa Waiver Permanent Program Act, Pub. L. No. 106-396, 114 Stat. 1637 (2000); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007); Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009, Pub. L. No. 110-329, 122 Stat. 3574 (2008); Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, 127 Stat. 198 (2013).

28. H.R. Rep. No. 104-828 (1996).

29. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208, 118 Stat. 3638, 3819 (2004).

30. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, § 711, 121 Stat. 266, 345 (2007).

31. When courts review the text of a law to determine congressional intent, courts will often apply a canon of statutory construction known as *expressio unius est exclusio alterius,* or more plainly, the expression-exclusion rule. This doctrine essentially provides that "expressing one item of [an] associated group or series excludes another left unmentioned is only a guide, whose fallibility can be shown

by contrary indications that adopting a particular rule or statute was probably not meant to signal any exclusion of its common relatives." United States v. Vonn, 535 U.S. 55, 65 (2002). *See also* Chevron U.S.A. Inc. v. Echazabal, 536 U.S. 73, 81 (2002) ("The canon depends on identifying a series of two or more terms or things that should be understood to go hand in hand, which is abridged in circumstances supporting a sensible inference that the term left out must have been meant to be excluded.") (citing E. Crawford, Construction of Statutes 337 (1940)); Ford v. U.S., 273 U.S. 593, 611 (1927) ("This maxim properly applies only when in the natural association of ideas in the mind of the reader that which is expressed is so set over by way of strong contrast to that which is omitted that the contrast enforces the affirmative inference that that which is omitted must be intended to have opposite and contrary treatment."). Under this canon of statutory construction, courts would likely read the aforementioned nine laws and conclude that Congress did not authorize face scans of Americans exiting the country.

32. *See* 5 U.S.C. § 553.

33. Office of Information and Regulatory Affairs, Executive Office of the President, RIN 1651-AB12, Collection of Biometric Data upon Entry to and Exit from the United States (2017), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201704&RIN=1651-AB12.

34. *Examining the Problem of Visa Overstays: A Need for Better Tracking and Accountability: Hearing Before the Senate Subcommittee on Border Security and Immigration* (July 12, 2017) (joint statement of Michael Dougherty, Assistant Secretary, Office of Strategy, Policy, and Plans, U.S. Customs and Border Protection; John Wagner, Deputy Executive Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection; and Louis A. Rodi, III, Deputy Assistant Director, National Security Investigations Division, Homeland Security Investigations, U.S. Immigration and Customs Enforcement) (as of June 2017), https://www.judiciary.senate.gov/imo/media/doc/07-12-17%20Dougherty-Wagner-Rodi%20Joint%20Testimony.pdf.

35. Electronic Privacy Information Center v. Department of Homeland Security, 653 F.3d 1, 8 (D.C. Cir. 2011). The court considered each exemption in turn and held that DHS needed to issue a notice and comment rule, or to claim an alternate exemption, to "cure the defect in its promulgation." *Id.* at 8.

36. Electronic Privacy Information Center, 653 F.3d at 6 ("overly abstract account of the change in procedure at the checkpoint elides the privacy interests").

37. *See, e.g.*, Frank Bajak & David Koenig, *Face scans for US Citizens Flying Abroad Stir Privacy Issues*, Associated Press (July 12, 2017), https://www.apnews.com/acf6bab1f5ab4bc59284985a3babdca4 (expressing privacy advocates' concerns about airport biometrics).

38. Electronic Privacy Information Center, 653 F.3d at 6 (to confirm the relevance of privacy issues, "we need look no further than [the agency's own] assurances"); *see, e.g.*, *CBP Meets with Privacy Groups to Discuss Biometric Exit*, U.S. Customs and Border Protection (Aug. 1, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-meets-privacy-groups-discuss-biometric-exit ("We are fully committed to meeting existing privacy laws and regulations while ensuring and safeguarding the privacy of all travelers."); *CBP Deploys Biometric Exit Technology to Chicago O'Hare International Airport*, U.S. Customs and Border Protection, (July 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-biometric-exit-technology-chicago-o-hare-international ("CBP remains committed to protecting the privacy of all travelers.").

39. *See* 73 Fed. Reg. 80 (Apr. 24, 2008).

40. Electronic Privacy Information Center, 653 F.3d at 7 (unless one of the other exemptions of the Administrative Procedure Act applies).

41. *Id.*

42. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4. ("[A]greements between CBP and the partner organization will guide opt-in/opt-out procedures. For some participating airlines, for instance, a traveler may request not to participate in the TVS and instead present credentials to airline personnel." It is not possible to evaluate the specific opt-in/opt-out procedures set forth in the referenced agreements, because the text of these agreements has not been made public.).

43. DHS stated in its June 2017 Privacy Impact Assessment that the Science and Technology Directorate "is generating a report identifying how each algorithm performed as a true positive rate, false positive rate, false match rate, and false non-match rate." Traveler Verification Service (TVS): Partner Process, *supra* note 4. However, in a more recent public meeting, in response to a question about testing for accuracy, a DHS spokesperson acknowledged it cannot measure impostor rates, stating: "On false positives it's hard because we wouldn't know." *See supra* note 25.

44. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4, 13 ("CBP requires an accuracy goal of 96% TAR for facial images acquired in an airport/seaport exit environment.").

45. *See supra* note 25.

46. *See, e.g.,* Patrick Grother, Mai Ngan & Kayee Hanaoka, NISTIR XXXX Draft, Ongoing Face Recognition Vendor Test (FRVT) Part I: Verification, NIST Figure 4 (Nov. 16, 2017), https://www.nist.gov/sites/default/files/documents/2017/11/16/frvt_report_2017_11_16.pdf (hereinafter "NIST FRVT 11-16-17") (illustrating the detection error trade-off between false nonmatch (False Reject) rates and false match (False Accept) rates). At a False Reject rate of 1 in 1,000 travelers, the 38 most recent algorithms studied produced an average False Accept rate of 9.4 percent. Lowering the rate of false rejects to 1 in 100,000 travelers raised the average rate of False Accepts to more than 27 percent. *Id.* (False Accept rates configured in typical operational systems). This is also intuitive. A face recognition system that allows everyone to board will have no false rejections, but it will allow 100 percent of impostors through the gate. In reverse, a system that rejects everyone would never permit an impostor to board but would have a False Reject rate of 100 percent.

47. *See* NIST FRVT 11-16-17, *supra* note 46.

48. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4.

49. NIST determined that the face scanning algorithms it evaluated generally had higher False Accept rates if the impostor's age, gender, and country of origin matched the demographics of the photo on file. *See* NIST FRVT 11-16-17, *supra* note 46. Figure, 101–160 (same sex and same region impostor pairs by age of impostor); NIST FRVT 11-16-17, *supra* note 46. Figure 18 ("These curves apply to zero-effort impostors . . . . [False Accept Rate] is higher for demographic-matched impostors.").

50. *See* NIST FRVT 11-16-17, *supra* note 46.

51. *See supra* note 25.

52. *Letter from Philip S. Kaplan, Chief Privacy Officer to Ms. Lisa Sotto, Chair of DHS Data Privacy and Integrity Advisory Committee (DPIAC)*, (Sept. 18, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/CBP%20Facial%20Recognition%20Tasking_FINAL%20_20170911.pdf ("I ask that the Committee address the following: . . . . Facial matching algorithms have often proven less accurate with certain demographic groups. What are business standard measurements for ensuring facial recognition accuracy across all demographics? Please provide recommendations . . . .").

53. *See supra* note 25.

54. NIST FRVT 11-16-17, *supra* note 46, Table 1.

55. For example, if the threshold were set at 95 percent, then if the traveler's face were calculated to have a 95 percent or higher similarity to the photo on file, the traveler would be considered a "match."

56. NIST FRVT 11-16-17, *supra* note 46, Figure 15. (Note that this section of the FRVT examines the algorithms' performance on mug shots, not visa images. The FRVT mugshot dataset is broken down explicitly by race, while the visa image dataset is not.)

57. It is important to note, however, that the earlier research concerned face *identification* systems, in which a single photo of an unknown person is compared against a large database of known persons to find a match. The current data emerging from NIST regarding bias concerns face *verification* systems, in which a photo of a person is compared against one photo of whom the system attempts to determine whether the person is who they claim to be or is where they are expected to be. This difference, as well as necessary differences in match thresholds set for the performance of the different types of systems, may explain the apparently contradictory results.

58. *See* Klare et al, *Face Recognition Performance: Role of Demographic Information*, IEEE (Oct. 9, 2012), *available at* http://ieeexplore.ieee.org/document/6327355/.

59. *See* Hannan Adely & Keldy Ortiz, *Protests Erupt at U.S. Airports over Ban on Refugees*, USA Today (Jan. 28, 2017), https://www.usatoday.com/story/news/nation-now/2017/01/28/protests-erupt-us-airports-over-ban-refugees/97201416/ ("Protests erupted at airports around the nation Saturday as Americans reacted in outrage to President Trump's sweeping order that banned people from seven Muslim-majority countries from entering the U.S. and suspended the nation's refugee program.").

60. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4, at 9 (June 12, 2017) (emphasis added).

61. *See U.S. Citizen Travel to International Regions*, U.S. Department of Commerce (Oct. 20 2017), https://travel.trade.gov/view/m-2016-O-001/index.html.

62. While the State Department already collects Americans' passport and foreign nationals' visa photos in its Consular Coordinated Database, DHS' routine use of face recognition on American citizens would be unprecedented. And without codified data disposal policies, DHS could use its face recognition deployment to create a database of high-quality, recent images of American travelers.

63. *CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport*, U.S. Customs and Border Protection (Oct. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint.

64. *Id.*

65. TSA Modernization Act, S. 1872, 115th Cong. (2017) https://www.commerce.senate.gov/public/_cache/files/e308d392-65e8-4f3a-828b-4c43a348b114/4C4E6267970C35B86B2BF21A5DA5529A.s.1872--tsa-modernization-act.pdf.

66. *Id.* § 216(2).

67. Border Security for America Act of 2017, H.R. 3548, 115th Cong. § 418(e)(3) https://homeland.house.gov/wp-content/uploads/2017/07/Bill-text.pdf.

68. *See* The International Justice and Public Safety Network (Nlets), Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, 2, 17 (June 30, 2011), *available at* https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf ("The potential harm of [face recognition] surveillance comes from its use as a tool of social control. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."); *see* Karen Gullo, *Surveillance Chills Speech—As New Studies Show—And Free Association Suffers*, Electronic Frontier Foundation (May 19, 2016), https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association.

69. *But see* Int'l Soc'y for Krishna Consciousness v. Lee, 505 U.S. 672 679–680, 685 (1992) (recognizing limitations to First Amendment protection for speech within and outside airport terminals).

70. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4, ("CBP is working with specified partners, such as commercial air carriers and airport authorities, who will collect the images of travelers and share the images with the

TVS, often through an integration platform or other vendor . . . . CBP recommends that its partners delete the matching results within 14 days . . . . However, once the images are shared with CBP, the airline or airport authority, along with their approved integrator or vendor, may choose to retain the newly-captured photos consistent with their contractual relationship with the traveler.").

71. *See* Alvaro M. Bedoya, *Why I Walked out of Facial Recognition Negotiations*, Slate (June 30, 2015), http://www.slate.com/articles/technology/future_tense/2015/06/facial_recognition_privacy_talks_why_i_walked_out.html ("Facial recognition lets companies identify you by name, from far away, and in secret. There's little you can do to stop it. You can't change your fingerprints or the unique dimensions of your face—not easily. And while you leave your fingerprints on only the things you touch, every time you step outside, your face appears, ready for analysis, in the video feeds and photographs of any camera pointing your way.").

72. *See* Traveler Verification Service (TVS): Partner Process, *supra* note 4, ("[S]igned Memoranda of Understanding (MOU) with CBP will govern [airlines'] retention practices").

73. *See* Justin Lee, *JetBlue, CBP Continue to Work with SITA in Biometric Exit Program*, Biometric Update (Sept. 23, 2017), http://www.biometricupdate.com/201709/jetblue-cbp-continue-to-work-with-sita-in-biometric-exit-program.

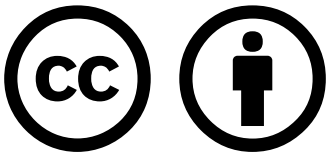
74. *See* Kate Modolo, *Delta Tests Next-Generation Biometric CBP eGates in Atlanta, JFK*, Delta News Hub (June 13, 2017), https://news.delta.com/delta-tests-next-generation-biometric-cbp-egates-atlanta-jfk.

75. *See* Lee Fang & Ali Winston, *Private Companies Look to Cash in as Homeland Security Brings Facial Recognition to U.S. Borders*, The Intercept (Nov. 29, 2017), https://theintercept.com/2017/11/29/facial-recognition-homeland-security-borders/.

76. *See supra* note 25.

77. *See* U.S. Department of Homeland Security, DHS/CBP/PIA-024(b), Privacy Impact Assessment Update for the Arrival and Departure Information System (ADIS) 2 (Apr. 28, 2017) ("ADIS consolidates entry, exit, and admission status information from several DHS components" in "near-real time"), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp024b-adis-april2017.pdf.

VIII. COPYRIGHT



The text of this report is made available under the Creative Commons Attribution 4.0 International license. This means you are free to:

- Share–copy and redistribute the material in any medium or format.
- Adapt–remix, transform, and build upon the material for any purpose, even commercially.

Under the following terms:

- Attribution–You must give the authors of this report appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- No additional restrictions–You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

For more information about this Creative Commons license, please visit creativecommons.org.

This report contains images that belong to other authors and that have been licensed for inclusion. All rights are reserved in any image found in this report, unless otherwise noted.

GEORGETOWN LAW
Center on Privacy & Technology