RESEARCH REPORT

BRENNAN CENTER FOR JUSTICE

Social Media Monitoring

How the Department of Homeland Security Uses Digital Data in the Name of National Security

PUBLISHED MAY 22, 2019

By Faiza Patel, Rachel Levinson-Waldman, Sophia DenUyl, and Raya Koreh

Brennan Center for Justice at New York University School of Law

Table of Contents

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform, revitalize, and — when necessary — defend our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
www.brennancenter.org

Sign up for our electronic newsletters at
www.brennancenter.org/signup

Introduction

The Department of Homeland Security (DHS) is rapidly expanding its collection of social media information and using it to evaluate the security risks posed by foreign and American travelers. This year marks a major expansion. The visa applications vetted by DHS will include social media handles that the State Department is set to collect from some 15 million travelers per year.[1] Social media can provide a vast trove of information about individuals, including their personal preferences, political and religious views, physical and mental health, and the identity of their friends and family. But it is susceptible to misinterpretation, and wholesale monitoring of social media creates serious risks to privacy and free speech. Moreover, despite the rush to implement these programs, there is scant evidence that they actually meet the goals for which they are deployed.

While officials regularly testify before Congress to highlight some of the ways in which DHS is using social media, they rarely give a full picture or discuss either the effectiveness of such programs or their risks. The extent to which DHS exploits social media information is buried in jargon-filled notices about changes to document storage systems that impart only the vaguest outlines of the underlying activities.

To fill this gap, this report seeks to map out the department's collection, use, and sharing of social media information by piecing together press reports, information obtained through Freedom of Information Act requests, Privacy Impact Assessments,[2] System of Records Notices (SORNs),[3] departmental handbooks, government contracts, and other publicly available documents.

In light of DHS's expanding use of social media monitoring programs, understanding the ways in which the department exploits social media is critical. Personal information gleaned from social media posts has been used to target dissent and subject religious and ethnic minorities to enhanced vetting and surveillance. Some DHS programs are targeted at travelers, both Americans and those from other countries. And while the department's immigration vetting programs ostensibly target foreigners, they also sweep up information about American friends, family members, and business associates, either deliberately or as a consequence of their broad scope.

Muslims are particularly vulnerable to targeting. According to a 2011 Pew survey (which was followed by a similar survey in 2017), more than a third of Muslim Americans who traveled by air reported that they had been singled out by airport security for their faith, suggesting a connection between being a devout Muslim and engaging in terrorism that has long been debunked.[4] A legal challenge to this practice is pending.[5] According to government documents, one of the plaintiffs, Hassan Shibly, executive director of the Florida chapter of the Council on American-Islamic Relations, was pulled aside for secondary screening at the border at least 20 times from 2004 to 2011.[6] He says he was asked questions like "Are you part of any Islamic tribes?" and "Do you attend a particular mosque?"[7] Shibly's story is hardly unique.[8]

Concerns about such screenings are even more urgent under the Trump administration, which has made excluding Muslims a centerpiece of its immigration agenda through policies such as the Muslim ban and implementation of "extreme vetting" for refugee and visa applicants, primarily those from the Muslim world.[9] A leaked DHS draft report from 2018 suggests that the administration is considering tagging young Muslim men as "at-risk persons" who should be subjected to intensive screening and ongoing monitoring.[10] If implemented, such a policy would affect hundreds of thousands of people.[11] DHS's social media monitoring pilot programs seem to have focused in large part on Muslims: at least two targeted Syrian refugees, one targeted both Syrian and Iraqi refugees, and the analytical tool used in at least two pilots was tailored to Arabic speakers.[12]

More generally, social media monitoring — like other forms of surveillance — will impact what people say online, leading to self-censorship of people applying for visas as well as their family members and friends. The deleterious effect of surveillance on free speech has been well documented in empirical research; one recent study found that awareness or fear of government surveillance of the internet had a substantial chilling effect among both U.S. Muslims and broader U.S. samples of internet users.[13] Even people who said they had nothing to hide were highly likely to self-censor online when they knew the government was watching.[14] As Justice Sonia Sotomayor warned in a 2012 Supreme Court case challenging the warrantless use of GPS tracking technology, "[a]wareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveals private aspects of identity is susceptible to abuse."[15]

DHS's pilot programs for monitoring social media have

been notably unsuccessful in identifying threats to national security.[16] In 2016, DHS piloted several social media monitoring programs, one run by ICE and five by United States Customs and Immigration Services (USCIS).[17] A February 2017 DHS inspector general audit of these pilot programs found that the department had not measured their effectiveness, rendering them an inadequate basis on which to build broader initiatives.[18]

Even more damning are USCIS's own evaluations of the programs, which showed them to be largely ineffective. According to a brief prepared by DHS for the incoming administration at the end of 2016, for three out of the four programs used to vet refugees, "the information in the accounts did not yield clear, articulable links to national security concerns, even for those applicants who were found to pose a potential national security threat based on other security screening results."[19] The brief does show that USCIS complied with its own rules, which prohibit denying benefits solely on the basis of public-source information — such as that derived from social media — due to "its inherent lack of data integrity."[20] The department reviewed 1,500 immigration benefits cases and found that none were denied "solely or primarily because of information uncovered through social media vetting."[21] But this information provided scant insights in any event: out of the 12,000 refugee applicants and 1,500 immigration benefit applicants screened, USCIS found social media information helpful only in "a small number of cases," where it "had a limited impact on the processing of those cases — specifically in developing additional lines of inquiry."[22]

In fact, a key takeaway from the pilot programs was that they were unable to reliably match social media accounts to the individual being vetted, and even where the correct accounts were found, it was hard to determine "with any level of certainty" the "authenticity, veracity, [or] social context" of the data, as well as whether there were "indicators of fraud, public safety, or national security concern."[23] The brief explicitly questioned the overall value of the programs, noting that dedicating personnel "to mass social media screening diverts them away from conducting the more targeted enhanced vetting they are well trained and equipped to do."[24]

The difficulties faced by DHS personnel are hardly surprising; attempts to make judgments based on social media are inevitably plagued by problems of interpretation.[25] In 2012, for example, a British national was denied entry at a Los Angeles airport when DHS agents misinterpreted his posting on Twitter that he was going to "destroy America" — slang for partying — and "dig up Marilyn Monroe's grave" — a joking reference to a television show.[26] As the USCIS pilot programs demonstrate, interpretation is even harder when the language used is not English and the cultural context is unfamiliar. If the State Department's current plans to undertake social media screening for 15

Case Studies: Using Social Media to Target First Amendment–Protected Activity

Several recent stories demonstrate how DHS has used social media to identify and target people for engaging in constitutionally protected activities.

>> **On March 6, 2019,** *The Nation* reported that Immigration and Customs Enforcement (ICE) was using Facebook to keep tabs on "anti-Trump" protests in New York City,[i] including an event organized by a congressman, to stand up against racism and xenophobia, as well as several "Abolish ICE" actions.[ii] Information about the protests, including the names of sponsoring organizations and the number of people who had signed up on Facebook to attend, was widely distributed within DHS.

>> **The same day,** NBC San Diego published slides from DHS Customs and Border Protection (CBP) titled "San Diego Sector Foreign Operations Branch: Migrant Caravan FY-2019, Suspected Organizers, Coordinators, Instigators and Media," dated January 9, 2019.[iii] The document is a surveillance target list with photographs of 59 people, 40 of whom were identified as U.S. citizens, and all of whom seemed to have some connection to advocacy for migrant caravans heading from Central America to the United States. Forty-three people, including 28 Americans, had "alerts" placed against their names. Many were tagged for questioning and stopped for additional screening by border agents. CBP also reportedly kept dossiers on all of them, including on an attorney with a legal center for migrants and refugees in Tijuana, Mexico.

Social media clearly played a part in identifying and tracking these individuals: pictures of several of them were taken from their social media profiles, and the "role" of three Americans was described in the DHS document as "administrator on caravan support Facebook page."[iv] The story triggered an immediate investigation by Rep. Bennie Thompson, the chair of the House Homeland Security Committee, into the possible misuse of CBP's authority.[v]

>> **On April 29, 2019,** *The Intercept* reported that an intelligence firm based in Virginia, LookingGlass Cyber Solutions, had compiled information on over 600 protests planned across the country in June 2018 in opposition to the Trump administration's policy of separating families at the border, and shared the data with DHS.[vi] The department characterized the information as "unsolicited" but nevertheless shared it widely with DHS employees, including ICE, and likely the FBI as well.[vii]

million travelers are implemented, government agencies will have to be able to understand the languages (more than 7,000) and cultural norms of 193 countries.[27]

Nonverbal communications on social media pose yet another set of challenges. As the Brennan Center and 34 other civil rights and civil liberties organizations pointed out in a May 2017 letter to the State Department:

> If a Facebook user posts an article about the FBI persuading young, isolated Muslims to make statements in support of ISIS, and another user "loves" the article, is he sending appreciation that the article was posted, signaling support for the FBI's practices, or sending love to a friend whose family has been affected?[28]

All of these difficulties, already substantial, are compounded when the process of reviewing posts is automated. Obviously, using simple keyword searches in an effort to identify threats would be useless because they would return an overwhelming number of results, many of them irrelevant. One American police department learned this lesson the hard way when efforts to unearth bomb threats online instead turned up references to "bomb" (i.e., excellent) pizza.[29] Natural language processing, the tool used to judge the meaning of text, is not nearly accurate enough to do the job either. Studies show that the highest accuracy rate achieved by these tools is around 80 percent, with top-rated tools generally achieving 70–75 percent accuracy.[30] This means that 20–30 percent of posts analyzed through natural language processing would be misinterpreted.

Algorithmic tone and sentiment analysis, which senior DHS officials have suggested is being used to analyze social media, is even less accurate.[31] A recent study concluded that it could make accurate predictions of political ideology based on users' Twitter posts only 27 percent of the time, observing that the predictive exercise was "harder and more nuanced than previously reported."[32] Accuracy plummets even further when the speech being analyzed is not standard English.[33] Indeed, even English speakers using nonstandard dialects or lingo may be misidentified by automated tools as speaking in a different language. One tool flagged posts in English by black and Hispanic users — like "Bored af den my phone finna die!!!!" (which can be loosely translated as "I'm bored as f*** and then my phone is going to die") — as Danish with 99.9 percent confidence.[34]

Crucially — as the USCIS pilot programs discussed above demonstrated — algorithms are generally incapable of making the types of subjective evaluations that are required in many DHS immigration programs, such as whether someone poses a threat to public safety or national security or whether certain information is "derogatory." Moreover, because these types of threats are difficult to define and measure, makers of algorithms will turn to "proxies" that are more easily observed. But there is a risk that the proxies will bear little or no relationship to the task and that they will instead reflect stereotypes and assumptions. The questioning of Muslim travelers about their religious practice as a means of judging the threat they pose shows that unfounded and biased assumptions are already entrenched at DHS. It would be easy enough to embed them in an algorithm.

Despite these serious shortcomings in terms of effectiveness and critics' well-founded concerns about the potential for targeting certain political views and faiths, DHS is proceeding with programs for monitoring social media.[35] The department's attitude is perhaps best summed up by an ICE official who acknowledged that while they had not yet found anything on social media, "you never know, the day may come when social media will actually find someone that wasn't in the government systems we check."[36]

The consequences of allowing these types of programs to continue unchecked are too grave to ignore. In addition to responding to particular cases of abuse, Congress needs to fully address the risks of social media monitoring in immigration decisions. This requires understanding the overall system by which DHS collects this type of information, how it is used, how it is shared with other agencies, and how it is retained – often for decades – in government databases. Accordingly, this paper maps social media exploitation by the four parts of DHS that are most central to immigration: Customs and Border Protection (CBP), the Transportation Security Administration (TSA), Immigration and Customs Enforcement (ICE), and United States Citizenship and Immigration Services (USCIS). It also examines DHS's cooperation with the Department of State, which plays a key role in immigration vetting.

Key Findings

While the ways in which these DHS units use social media vary, our review identified eight common threads.

1. Social media information is collected from travelers, including Americans, even when they are not suspected of any connection to illegal activity.

People planning to travel to the United States are increasingly being asked to provide social media identifiers, such as their Twitter or Instagram handles, enabling the creation of a registry of their online postings. In December 2016, DHS began asking the travelers who come to the United States from countries covered by the Visa Waiver Program — some 23.6 million annually, primarily from Western Europe — to voluntarily provide their social media identifiers.[37] In May 2017, the State Department, as part of implementing the Muslim ban executive order, began requiring some categories of visa applicants — estimated at 65,000 applicants annually — to provide a list of the identifiers they had used on social media platforms within the previous five years.[38] In March 2018, the State Department started to ramp up its efforts, proposing a new rule that would collect social media identifiers from every visa applicant — i.e., the 15 million people who apply for visas each year.[39] The proposal was approved in April 2017, with minor privacy–related changes.[40]

Social media data can also be collected via searches of electronic devices, which DHS carries out — without suspicion of criminal activity — on both American and foreign travelers. The department claims the authority to undertake warrantless searches of these devices not just at points of entry but also in areas in the broad vicinity of the border.[41] These searches are conducted primarily by CBP and ICE. While ICE does not report statistics on these searches, CBP does. Its searches of travelers' electronic devices at ports of entry have been steadily increasing over the past several years. In fiscal year 2015, CBP searched the devices of 8,503 travelers.[42] By fiscal year 2017, this number had gone up to 30,200 — an increase of over three and a half times.[43] According to ABC News, 20 percent of these searches are carried out on American travelers.[44]

Finally, through contracts with various private companies, DHS acquires massive commercial databases of online information, including social media data.[45] Unlike the direct collection of social media handles by DHS and the State Department, there is no assurance that an individual will be accurately connected to a social media profile. The difficulty of matching people to profiles was a major shortcoming of automated monitoring tested by the pilot programs discussed above.[46]

2. Social media checks extend to travelers' family, friends, business associates, and social media contacts.

When DHS checks the social media of someone trying to obtain permission to come to the United States or someone already at or near the border, it inevitably picks up information about people with whom they interact. For example, ICE agents searching a traveler's smartphone at or near the border can download the entirety of her Facebook and Twitter accounts and go through them later.[47]

In addition, CBP agents conducting social media checks for people applying for visa waivers (available to the citizens of 38 countries) can examine not only the applicant's posts but those of the people who interacted with her on social media (even if uninvited), and may retain information so long as the agent believes it is "relevant" to the waiver decision.[48] The program also allows agents to proactively identify an applicant's secondary and tertiary contacts who might "pose a potential risk to the homeland" or "demonstrate a nefarious affiliation on the part of the applicant."[49] Examining contacts and networks may make sense when pursuing someone who is suspected of wrongdoing. But applying this technique to people who are simply seeking to travel opens the door to fishing expeditions for information that can easily be misinterpreted.

Automated analytical tools used by DHS combine social media with other types of information to identify and map possible associations among people and organizations. ICE and CBP both use data systems developed by the data mining[50] company Palantir Technologies, Inc., that are equipped with tools to analyze social networks.[51] However, the reliability of the information ingested by these systems is not verified; DHS has exempted them from the relevant requirements of the Privacy Act, and there are functionally

no mechanisms for the individuals whose information is included to challenge the accuracy of the data.[52] According to reports from watchdog groups and the press, these systems are being used by ICE to identify individuals for deportation.[53]

These data sets are also used by DHS to undertake broader trend, pattern, and predictive analyses, through a number of systems that are described in this paper.[54] While the privacy impact assessments for these systems often identify the sources of information used in these analyses, there is almost no publicly available information regarding what types of trends or patterns DHS is seeking to identify or how social media information fits into these types of analyses.

3. DHS frequently uses social media information for vague and open-ended evaluations that can be used to target unpopular views or populations.

Our review showed that in many instances — including the Visa Waiver Program and warrantless searches at the border by CBP and ICE — DHS personnel are charged with examining social media to identify information relating to undefined "national security" risks or concerns.[55] Publicly available documents do not indicate what type of information might be regarded as indicative of a national security risk, and it has been reported that at least some agents are uncertain about what type of information would be considered to be suggestive of a national security risk.[56] While agents obviously must have some flexibility to make judgments, the breadth of discretion combined with weak safeguards opens the door for discrimination based on political or religious views.

Social media information forms part of the data set that DHS uses to assign risk assessments to individual travelers through CBP's Automated Targeting System (ATS). These assessments are highly consequential because they determine who is allowed to enter the country and what level of questioning they are required to undergo.[57] But there is no publicly available information about the accuracy, effectiveness, or empirical basis of risk assessments.[58] In fact, the information that goes into one's risk assessment need not be "accurate, relevant, timely, [or] complete," as DHS exempted ATS from these Privacy Act requirements.[59] This is particularly troubling because in other settings, such as the criminal justice system, risk assessments have been shown to disproportionately impact minorities.[60]

For example, as of at least 2017, DHS compares refugee and asylum applicant information from social media and other sources against the information provided by an applicant to identify any inconsistencies. Such social media checks are, however, performed only on select populations of asylum seekers and refugees. With the exception of Iraqis and Syrians, these applicant populations have not been publicly identified.[61] However, one prominent refugee organization reported in 2018 that these measures are applied to refugee applicants from the Muslim countries of Egypt, Iran, Iraq, Libya, Mali, Somalia, South Sudan, Sudan, Syria, and Yemen, as well as North Korea.[62] All of the countries covered by the Trump Muslim ban are on this list.

4. DHS is continuously monitoring some people inside the United States and plans to expand these efforts.

DHS is increasingly implementing programs to continuously monitor people inside the United States, where freedom of speech, association, and religion are constitutionally protected. For example, using social media and other sources, ICE monitors students who enter the United States planning to study a "nonsensitive" topic and later change to one the State Department categorizes as "sensitive" (e.g., nuclear physics, biomedical engineering, or robotics).[63] ICE's Overstay Lifecyle Program targets visitors from a number of unidentified countries to uncover derogatory information for ongoing monitoring, including through social media. And ICE's planned Visa Lifecycle Vetting Initiative would keep tabs on 10,000 foreign visitors flagged as "high risk" by monitoring their social media activity.[64] As noted earlier, a draft CBP report recommended continuously monitoring young Muslim men while they were in the United States. If implemented, this discriminatory policy would affect hundreds of thousands of people.[65]

5. DHS is increasingly seeking and using automated tools to analyze social media.

While the full scope of DHS's efforts to use algorithms is not known, our research shows that at least three branches of DHS — CBP, ICE, and USCIS — now use automated tools to analyze social media information, either alongside other data or by itself. For instance, CBP's Analytical Framework for Intelligence has automated analytic capabilities, developed by Palantir, to identify "non-obvious" links among

data points, people, and organizations.[66] Similarly, ICE has contracted with the data mining firm Giant Oak to continuously monitor, aggregate, and analyze social media data to provide ICE with prioritized rankings of leads for its overstay enforcement initiatives.[67] The push toward automation raises concerns given the poor track record of automated systems trying to make complicated judgments and the ambiguity of many social media posts, as amply demonstrated by the USCIS pilot programs.[68]

6. Social media information collected for one purpose is used by DHS in a range of other contexts, increasing the likelihood of misinterpretation.

The difficulty of interpreting Facebook posts and offhand tweets likely only worsens as they are captured in numerous databases and systems and used for a range of analyses. Empirical research shows that as data becomes further and further removed from the context and aim of its original collection, it is less likely to be useful for secondary analysis.[69]

The DHS data architecture is a vast, ambiguous, and highly interconnected system in which social media is available for several types of secondary analyses. For example, when someone applies for a visa waiver to visit the United States, that person is asked to provide his or her social media identifiers, such as a Twitter handle.[70] The CBP officer who evaluates the applicant's tweets conducts an individualized assessment and has available a range of biographical information that provides context for what the applicant has said on social media. We know from DHS's own pilot programs discussed above that this type of analysis is mostly unproductive. These problems are exacerbated when the information is used for secondary analyses. The social media identifiers as well as information obtained from CBP border searches also make their way into the Automated Targeting System, where the information can be used to generate "risk assessments" for other individuals altogether.[71] The information in ATS also feeds into numerous other data systems and is used, for example, by TSA to prescreen travelers and to vet visa applicants and people applying for immigration benefits.[72] When already difficult-to-interpret information is taken out of context, the risks of misunderstandings only increase.

7. Social media information collected by DHS is shared with other law enforcement and security agencies under broad standards.

The past two decades have seen a proliferation in information-sharing arrangements among various government agencies and even with foreign governments. With stringent standards and controls, such arrangements can serve valid purposes. But sharing information about people's political and religious views, especially when gleaned from the ambiguous realms of social media, only expands the possibility of abuse and inappropriate targeting. For example, the CBP program to track and interrogate journalists and activists at the southern border, discussed earlier, was apparently carried out in cooperation with Mexican authorities.[73] The target list showed that Mexican authorities had deported seven people and arrested three others, including nationals of the United States, Honduras, and Spain.[74] These actions by Mexico, which raise serious concerns about the targeting of political speech and organizing, could well have been the result of the sharing of information by CBP. Reporting also indicates that agents from the San Diego office of the Federal Bureau of Investigation (FBI) were involved in the operation, raising concerns about whether CBP intended that the FBI target the Americans on the list for surveillance.[75]

Unfortunately, DHS programs generally have low standards for sharing highly personal information, such as that found on social media, and the standards do not differentiate between Americans' information and that of people from other countries. This information can easily be shared with entities ranging from the Department of State, the FBI, and congressional offices to foreign governments and Interpol. For example, data obtained from CBP searches of travelers' electronic devices at the border, which can include the full contents of these devices, can be shared with federal, state, tribal, local, or foreign governmental agencies or multilateral government organizations when CBP believes the information could assist enforcement of civil or criminal laws.[76] ICE, too, can disseminate any device information "relating to national security" to law enforcement and intelligence agencies.[77] Information from ICE's LeadTrac system, which is used to vet and manage leads of suspected overstayers and status violators and includes social media information, can be shared with any law enforcement authorities engaged in collecting law enforcement intelligence "whether civil or criminal."[78]

Information shared with agencies can proliferate even further because DHS frequently does not place limits on re-dissemination. USCIS's Alien Files system, for exam-

ple, stores social media information on people applying for immigration benefits (such as a change of status from one type of visa to another, or naturalization) but does not seem to limit re-dissemination.[79] In addition, sometimes databases ingested by DHS do not adequately reflect the dissemination restrictions of the original system. For example, the Department of State databases for visa applications include some modest sharing restrictions, but it does not appear that these restrictions are honored when the State Department information is ingested into CBP's systems.[80]

8. DHS systems retain information for long periods, sometimes in violation of the department's own rules.

While databases are part of how DHS carries out its functions, its extended retention of large pools of personal information untethered to any suspicion of criminal activity raises serious concerns about privacy risks and misuse of data.[81] In 1974, the Church Committee's report on surveillance abuses by U.S. intelligence agencies warned: "The massive centralization of . . . information creates a temptation to use it for improper purposes, threatens to 'chill' the exercise of First Amendment rights, and is inimical to the privacy of citizens."[82] The accumulation of data intrudes on people's privacy by allowing government authorities to know the details of their personal lives. These risks have only become greater because data — including what we say on social media — can be so readily combined and searched.

To manage these types of risks, as well as to ensure that inaccurate and out-of-date information is weeded out, DHS's data systems incorporate rules that limit the retention of information beyond a specified time frame. Unfortunately, these retention limits are often not carried over from one DHS database to another, so that once social media information is shared (often automatically), it is kept in the receiving database for longer than intended.

For example, CBP's ATS stores a range of data from various sources, and as DHS admits, it fails to "consistently follow source system retention periods," instead retaining most information for 15 years by default.[83] This means that information stored in ATS, such as Visa Waiver Program applications that include applicants' social media identifiers and are supposed to be kept for no more than three years, may be retained for five times that long.[84]

The lack of respect for retention rules is not limited to particular programs either. Since 2015, data from ATS has been copied in bulk to go into the consolidated DHS-wide Data Framework, a new system that is expected to play an enormous role in the agency's operations.[85] Because ATS does not abide by source restrictions, the Data Framework likely does not comply with such restrictions either, and will instead rely on data that may be outdated, incorrect, or already deleted from the source system.[86]

Moreover, some systems have long retention periods by design. USCIS's Alien Files — which contain the official record of an individual's visa and immigration history and may include social media information — are stored for 100 years after the individual's date of birth.[87] Long retention periods for social media information further exacerbate the risk of misinterpretation. A social media post from 2007 may take on a whole new meaning by 2022, and even more so decades later.

The appendix at the end of this report contains further details on the retention of information in DHS systems.

As the findings above show, DHS incorporates social media into almost all aspects of its immigration operations, from visa vetting to searches of travelers to identifying targets for deportation. Hundreds of thousands or even millions of people, including Americans, are caught up in this net. While some of what the department is doing may well be justified, the scope of its monitoring activities is hidden behind jargon-filled notices and only rarely evaluated. Policymakers and the public need to know the when, why, what, and how behind DHS social media monitoring so that they can make informed judgments about the risk, efficacy, and impact of these initiatives.

Customs and Border Protection

Customs and Border Protection (CBP) is the arm of DHS charged primarily with securing the nation's borders. CBP uses social media information as part of its review of applications to enter the United States. Social media information is also part of CBP's preflight risk assessments and watch list screening and is used to develop broader intelligence analysis products.[88] CBP's reliance on social media to perform these critically important functions is misplaced. DHS's own pilot programs show that social media information is rarely a reliable basis for making judgments. And the vague standards used to assess social media invite discrimination against certain individuals, such as those involved in protest and activism and Muslim travelers. Unreliable social media information is easily shared within and beyond DHS, exposing personal information to a range of actors and increasing the risk that the data will be used out of context.

1. Visa Vetting

A. Visa Waivers (ESTA Program)

DHS, in consultation with the State Department, administers the Visa Waiver Program, through which citizens of 38 mainly Western European countries can travel to the United States for business or tourism without obtaining a visa.[89] In fiscal year 2017, more than 23 million travelers came to the United States through the program.[90] Travelers from these countries who wish to obtain a visa waiver must complete a mandatory online application on the Electronic System for Travel Authorization (ESTA).[91] The information provided through ESTA is vetted against security and law enforcement databases to determine whether applicants are eligible to travel under the program and to ensure they do not pose a law enforcement or security risk.[92] These travelers are also continually screened in real time.[93]

Social media information is increasingly being used in this process to vet for national security concerns, although only one American was killed in a terrorist attack by a traveler on the Visa Waiver Program between 1975 and 2017, according to a study by the Cato Institute.[94] While social media checks were previously used by CBP, the agency added a new question to the forms in December 2016, asking all applicants to voluntarily provide their social media identifiers, such as any usernames and platforms used.[95] If applicants choose to provide identifying information, officers may use it to locate their profiles and accounts when the initial screening indicates "possible information of concern" or "a need to further validate information."[96]

Regardless of whether ESTA applicants have chosen to provide their social media identifiers, CBP officers may still choose to manually check their accounts; it does not appear that the officer must first make a finding of "possible information of concern" or "a need to further validate information" in order to do so.[97] In such instances, in addition to the interpretive issues identified above, it is unclear how CBP officials confirm that they have correctly connected the applicant to the right social media accounts. This was a recurring problem in the pilot programs discussed previously.[98]

Publicly available documents do not indicate what types of postings on social media would be considered by CBP to be indicative of a national security threat.[99] But the vagueness of the standards creates the risk that innocuous social media activity will be used as a means of excluding people of certain political or religious beliefs. In a nod to this risk, CBP documents state that information from social media "will not" be the sole basis upon which CBP denies someone entry to the United States.[100] But this restriction may not be particularly effective because CBP could combine one questionable or weak social media "find" with virtually any other information to deny a visa waiver. For example, CBP and other arms of DHS are not permitted to use ethnicity as the sole basis for suspecting an individual is undocumented, but ethnicity combined with other factors — such as appearing nervous — has been used to stop people on suspicion of undocumented status.[101]

The social media check can also extend to associates who posted on or interacted with an applicant on their social media profile, which could include Americans and other contacts living in the United States if "relevant to making an ESTA determination."[102] In addition, CBP uses "link analysis" to proactively identify contacts of applicants (e.g., friends, followers, or "likes"), as well as the applicant's secondary and tertiary contacts who might "pose a potential risk to the homeland" or "demonstrate a nefarious affiliation on the part of the applicant."[103] CBP has no qualms about drawing adverse conclusions from things that third

parties have posted — rather, it "presumes" that at least some of the information posted on the applicant's site, including from third parties, is accurate because "individuals generally have some degree of control over what is posted on their sites."[104]

Thus, even if nothing posted by the applicant suggests he or she poses a risk, CBP could still potentially deny a visa waiver based in part on concerns related to a tweet posted by a "friend" or follower, who could easily be someone the applicant does not even know. Unfortunately, unlike some other DHS programs, there is no opportunity for the applicant to address or explain the inferences that CBP draws from their social media.

DHS rules require officers to collect only the minimum personally identifiable information "necessary for the proper performance of their authorized duties."[105] But according to the 2017 privacy audit of ESTA, DHS's Privacy Office could not verify whether CBP was adhering to this requirement.[106] Other significant controls — that DHS officers are limited to reviewing publicly available information and must use official DHS accounts to conduct such checks — can be circumvented using a technique called "masked monitoring."[107] But the circumstances triggering such monitoring and the applicable rules are not publicly available.[108]

All social media information about those applying for visa waivers (and potentially about their friends and contacts), as well as other data from ESTA applications and related paperwork, is stored in CBP's Automated Targeting System (ATS).[109] CBP agents use the information in ATS to assign risk assessments to travelers, which can impact their vetting and questioning at the border. ATS risk assessments and other analyses also feed into a number of watch lists, such as the FBI's Terrorist Screening Database and TSA Watch Lists, as well as analytical products on trends and threats.[110] In other words, what a person says on social media, which is often context-specific and ambiguous to outsiders, feeds into every aspect of CBP's work and that of DHS more broadly.

ESTA information — about applicants and their friends and families — is also disseminated widely to a broad range of entities, including the Departments of Justice and State.[111] As of December 2018, the National Vetting Center (NVC), a presidentially created clearinghouse and coordination center for vetting information, has been involved in ESTA's work.[112] CBP is required to regularly share ESTA application data with a number of agencies involved in the NVC, including the CIA and the Department of Defense, to be compared against the holdings of those agencies.[113] Beyond the bulk sharing with the NVC, ESTA information sharing with other agencies is not confined to situations in which there is an indication that the traveler has violated the law. Rather, it can take place simply when DHS determines that the information "would assist in the enforcement of civil or criminal matters."[114] In addition, DHS and the National Counterterrorism Center (NCTC), which is charged with collecting counterterrorism intelligence, have entered into a memorandum of understanding allowing DHS to disclose the entire ESTA data set to the NCTC.[115] This data set would go far beyond information about individuals suspected of any connection to terrorism and would include information gathered during routine interactions with the public (e.g., screening travelers, reviewing immigration benefit applications, issuing immigration benefits).[116]

In sum, the ESTA program demonstrates that CBP collects highly personal information available on social media about those applying for visa waivers and the people in their networks. CBP uses this information, which is highly contextual and subject to interpretation, to decide whether an individual poses an undefined "security risk." All of this information is stored in DHS databases for years and potentially used for a range of purposes, often far removed from the purpose of the initial collection.[117] The information is shared in bulk with the NCTC, and with other law enforcement agencies as long as it could be of "assistance" to them, creating risks to privacy and freedom of speech and association.

B. Visa Applications

The State Department has ramped up its collection of social media information from people applying for visas, which it shares with DHS to be vetted using ATS.[118] In May 2017, the State Department began requiring some categories of visa applicants — estimated at 65,000 per year — to provide the identifiers they used on all social media platforms within the previous five years.[119] It seems likely that this move was aimed primarily at travelers from the Muslim ban countries; the Federal Register notice announcing the rule change indicated that it was being implemented as part of the Muslim ban, and the notice's estimate of the number of travelers who would be affected by the change approximately matched those affected by the overall ban.[120]

In March 2018, the State Department sought to vastly expand the collection of social media identifiers to the approximately 15 million people who apply for visas each year.[121] The Office of Management and Budget (OMB) approved the proposal in April 2019, which means the State Department will begin collecting from nearly all visa applicants their social media identifiers associated with any of 20 listed social media platforms, more than half of which are based in the United States (Facebook, Flickr, Google+, Instagram, LinkedIn, Myspace, Pinterest, Reddit, Tumblr, Twitter, Vine, and YouTube).[122] The other platforms are based in China (Douban, QQ, Sina Weibo, Tencent Weibo, and Youku), Russia (Vkontakte), Belgium (Twoo), and Latvia (Ask.fm).[123] Applicants will also have the option of providing identifiers for platforms not included on the list.[124]

As with the DHS social media collection programs described throughout this paper, there is limited information on what the State Department's review of applicants' social media activity will entail. We only know that it is meant to enable consular officers to confirm applicants'

identity and adjudicate their eligibility for a visa under the Immigration and Nationality Act.[125] While the notice does state that "the collection of social media platforms and identifiers will not be used to deny visas based on applicants' race, religion, ethnicity, national origin, political views, gender, or sexual orientation," this restriction is easily circumvented: a social media post revealing an applicant's religious or political affiliation may not alone justify denial, but other information in his or her file could easily be used as a pretext, particularly given the broad discretion exercised by consular officials.[126] According to the statement supporting the notice, consular officers will also be directed not to request passwords, violate the applicant's privacy settings or the platforms' terms of service, or engage with the applicant on social media; to comply with State Department guidance limiting the use of social media; and to avoid collecting third-party information.[127]

The State Department's expected trove of information will likely be used for a variety of purposes beyond visa vetting. Social media identifiers collected by the State Department will be stored in the Consolidated Consular Database, which is ingested into ATS and becomes available to DHS personnel.[128] Further, that information will be used in coordination with other department officials and partner U.S. government agencies.[129] Indeed, numerous other agencies have access to the visa records system in which applicants' social media information will be stored, and — along with foreign governments — can obtain information from the system.[130]

In sum, the State Department's collection of social media information, which already includes 65,000 visa applicants (likely those targeted by Trump's Muslim ban), is on track to begin creating a registry that will include 15 million people after the first year alone. Not only will this information be used by the State Department in undefined ways to make visa determinations, but it will be yet another source of personal information that is funneled into DHS's many interconnected and far-reaching systems.[131]

2. Warrantless Border Searches

CBP conducts warrantless searches at the border on a wide variety of electronic devices, such as phones, laptops, computers, and tablets, many of which are likely to result in the collection of social media information. According to CBP, these searches are meant to help uncover evidence concerning terrorism and other national security matters, criminal activity like child pornography and smuggling, and information about financial and commercial crimes.[132] However, CBP documents also describe these searches as "integral" to determining an individual's "intentions upon entry" and to providing other information regarding admissibility.[133]

While some of these searches are conducted manually, CBP also has technical tools for extracting information from these devices, potentially including information stored remotely.[134] It has purchased powerful handheld Universal Forensic Extraction Devices (UFEDs), developed by the Israeli company Cellebrite, which can be plugged into phones and laptops to extract in a matter of seconds the entirety of a device's memory, including all data from social media applications both on the device and from cloud-based accounts like Facebook, Gmail, iCloud, and WhatsApp.[135]

Searches by CBP of travelers' electronic devices at ports of entry have increased dramatically over the past several years. In fiscal year 2015, 8,503 people had their devices searched.[136] By fiscal year 2017, the number had reached 30,200 — an increase of over three and a half times.[137] According to CBP, these searches do not require a warrant, due to "a reduced expectation of privacy associated with international travel."[138] Both American and foreign travelers are subjected to these warrantless searches.[139] In 2017, 10 U.S. citizens and one green card holder filed suit challenging warrantless searches of electronic devices at the border.[140] The complaint highlights the intrusiveness of these searches, both for the person being searched and for the traveler's family, friends, and acquaintances, given the many contact lists, email messages, texts, social media postings, and voicemails that cellphones and laptops often contain.[141]

Under a January 2018 directive, CBP is permitted to conduct two types of searches: "basic" and "advanced," both of which would allow collection of information from social media.[142] The 2018 directive changed CBP's previous, more permissive rule, likely as a partial and belated response to a 2013 federal court decision, *United States v. Cotterman.* In that case, a federal court of appeals held that the fact that a device was seized at a border did "not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information," and required that officers have reasonable suspicion of criminal activity to conduct forensic searches of electronic devices.[143] ICE continues to operate under the older regime, however, and CBP is permitted to refer travelers to ICE at any stage of the inspection process, at which point ICE's more permissive policy would apply.[144]

Under CBP's new rules, a basic search permits an agent to view information that "would ordinarily be visible by scrolling through the phone manually."[145] No suspicion of criminal wrongdoing or national security risk is required for basic searches. For either type of search, agents are prohibited from "intentionally" accessing data that is "solely stored remotely"; only information that is "resident on the device and accessible through the device's operating system or through other software, tools, or applications" may be viewed.[146] CBP officers are supposed to disable network connectivity or request that the traveler do so (e.g., by switching to airplane mode) prior to the search; they are also supposed to conduct the search in the presence of the

traveler in most circumstances, though the individual will not always observe the actual search.[147]

Despite these new guidelines, CBP agents will probably still be able to access social media information during a search. If a traveler has social media data downloaded onto his or her device or cached in some way, it is likely accessible even if connectivity is turned off.[148] For example, if a traveler was scrolling through a Twitter or Facebook feed prior to being selected for a search, any loaded data, such as his or her newsfeed, would be accessible on the user's phone or laptop.

The officer may also request that the traveler provide any passcodes needed to access the contents of a device.[149] Although a traveler can refuse to provide a code, CBP may then keep the device in order to try to access its contents by other means.[150] U.S. citizens must be admitted to the country even if they do not provide passcodes, though their phones may still be held for five days or longer.[151] Noncitizens, however, including visa holders and tourists from visa waiver countries, may be denied entry entirely.[152]

An advanced search occurs when an officer connects an electronic device to external equipment, via a wired or wireless connection, to review, copy, or analyze its contents.[153] Advanced searches are highly intrusive, and the tools that CBP has purchased allow it to capture all files and information on the device, including password-protected or encrypted data.[154]

Officers are authorized to perform advanced searches if there is reasonable suspicion that one of the laws enforced or administered by CBP has been violated or if there is a "national security concern."[155] In creating an exception for "national security concerns," DHS policy departs from the *Cotterman* decision, which required reasonable suspicion for all forensic searches. While DHS does not define what constitutes a national security concern, national security is an expansive term that could easily swallow up the requirement of suspicion for these highly intrusive searches. The examples listed in the 2018 privacy impact assessment suggest that national security searches will be based on watch lists. However, this category includes not just lists kept by the government — primarily the FBI and DHS — but other lists as well, such as unspecified "government-vetted" watch lists and a "national security-related lookout in combination with other articulable factors as appropriate."[156] And, of course, these examples are not exhaustive, leaving open the possibility that agents will use the cover of national security to undertake forensic searches even when there is no relevant watch list.

Following both basic and advanced searches, the officer enters notes about the interaction, including "a record of any electronic devices searched," into TECS, CBP's primary law enforcement system.[157] This typically includes device details, the type of search performed (basic or advanced), and the "officer's remarks of the inspection."[158] CBP may detain a device, or copies of the information it contains, for up to five days, although it can keep a device longer when there are unspecified "extenuating circumstances."[159] If there is no probable cause to seize and retain a device or the information it contains, the device must be returned to the traveler and any copies destroyed.[160] However, CBP may retain without probable cause any information "relating to immigration, customs, and other enforcement matters," which seems to allow it to essentially circumvent the probable cause requirement.[161] For instance, information that could be considered useful for determining whether an individual may be permitted to travel to the United States could be stored in the individual's Alien File, 100 years after their date of birth.[162]

Any information that is copied directly from an electronic device during an advanced search (presumably based on probable cause) is stored in ATS, which allows agents to further analyze information collected by comparing it against various pools of data and applying ATS's analytic and machine learning tools to recognize trends and patterns.[163] CBP may disclose information from electronic device searches to other agencies, both within and outside DHS, if it is evidence of violation of a law or rule that those agencies are charged with enforcing.[164]

Notably, a December 2018 DHS inspector general report concluded that CBP had not been following its own standard operating procedures prior to the implementation of the new rules.[165] The report, which was based on a review of CBP's electronic device searches at ports of entry from April 2016 to July 2017, found that officers frequently did not document searches properly, that they consistently failed to disable network connection prior to search (specifically for cell phones), and that the systems used and data collected during searches were in many cases not adequately managed and secured.[166] For instance, officers often failed to delete travelers' information stored on the thumb drives used to transfer data to ATS during advanced searches.[167] The report also found that CBP had no performance measures in place to assess the effectiveness of its forensic searches of electronic devices.[168]

The 2018 directive instructed CBP to develop and periodically administer an auditing mechanism to ensure that border searches of electronic devices were complying with its requirements.[169] However, the agency has published neither the requirements nor the results of the audits. In February 2019, the Electronic Privacy Information Center (EPIC) sued for the release of this information.[170]

Even if the rules are operating as intended, they may also be applied discriminatorily. For instance, Muslim travelers have long been singled out for additional scrutiny because of their faith,[171] which President Trump and his administration have repeatedly and inaccurately connected with "terrorism."[172] Just months after the new policy was issued, the Council on American-Islamic Relations (CAIR) sued CBP on behalf of a Muslim American woman whose iPhone was seized and its contents imaged when she came home from Zurich.[173] She was also questioned about her travel history and whether she had ever been a refugee.[174] The

lawsuit asked CBP to explain what suspicion warranted the forensic search and demanded deletion of the information seized.[175] The government quickly settled, agreeing to delete the data it had seized.[176]

In sum, CBP is increasingly deploying its claimed warrantless border search authority to search the electronic devices of both visitors and American travelers. Basic searches conducted without any suspicion of wrongdoing can result in the scrutiny of travelers' social media information. Advanced searches will result in the collection of huge amounts of personal information, including from social media, about both the person whose device is being searched and that person's contacts. CBP has stated that it has this broad authority in order to help uncover information related to terrorism and criminal activity and to determine admissibility. But there is little indication in public documents as to what type of content officers should be looking for, especially in deciding whether a traveler can enter the country, allowing for unfocused fishing expeditions. And these searches are not subject to even minimal safeguards—such as an instruction to avoid making decisions based solely on social media or a prohibition on profiling. And the search is just the start. CBP is permitted to retain information relating to immigration, customs, or other enforcement matters it finds useful, including a copy of the contents of phones and laptops; as discussed further below, the agency may also further analyze the information using unknown tools and algorithms.[177]

3. Searches Pursuant to Warrant, Consent, or Abandonment

CBP also collects information from electronic devices in three other situations:

- When it has a warrant authorized by a judge or magistrate based on probable cause;[178]
- When an officer finds an abandoned device that he or she suspects "might be associated with a criminal act" or was found in "unusual circumstances" (such as between points of entry in the "border zone,"[179] the area within 100 miles of any U.S. boundary in which Border Patrol claims authority to conduct immigration checks[180]); and
- When the owner has consented.[181]

According to CBP, once the information is determined to be "accurate and reliable," it is used to support the agency's border enforcement operations and criminal investigations.[182] DHS materials note that such information is "typically" used only to corroborate evidence already in the agency's possession.[183]

Agents are explicitly allowed to collect information stored in the cloud when spelled out in a warrant or when the owner consents, but it is not clear whether cloud data can be accessed from abandoned devices.[184] A CBP officer or agent can submit devices found in one of the aforementioned scenarios for digital forensic analysis, which is usually undertaken by a team of agents at the intelligence unit for the relevant Border Patrol sector.[185]

If the CBP agent determines after conducting one of these examinations that an electronic device holds information that is "relevant" to the agency's law enforcement authorities, the agent may load all information into a stand-alone information technology system for analysis.[186] This is the rare database that "*may not* be connected to a CBP or DHS network."[187] The tools built into these stand-alone systems allow CBP to perform various analyses on the collected information.[188] One system, ADACS4, is used to analyze data from electronic devices in order to discover "connections, patterns, and trends" relating to "terrorism" and the smuggling of people and drugs, as well as other activities that threaten border security.[189]

CBP retains information associated with arrests, detentions, and removals, including data obtained from electronic devices, for up to 75 years. Even information that does not lead to the arrest, detention, or removal of an individual — and that may be completely irrelevant to DHS's duties — may be stored for 20 years "after the matter is closed."[190]

The information collected by CBP from electronic devices is frequently disseminated within DHS and to other federal agencies or state and local law enforcement agencies with a need to know, and less frequently to foreign law enforcement partners.[191] In addition to sharing with agencies investigating or prosecuting a violation of law, CBP may also share information for unspecified counterterrorism and intelligence reasons.[192]

The CBP search authorities detailed above allow the collection of social media information. While the warrant and consent authorities seem reasonably cabined, the authority to search abandoned devices is quite expansive, especially if it is read to apply to all devices found within 100 miles of U.S. land or coastal borders, where two-thirds of Americans live.[193] It is not clear why the information from these categories of devices is held in a separate database, unconnected to other DHS systems. As with other collection programs, CBP uses the social media information it collects to conduct trend or pattern analyses and shares it with other agencies, raising concerns about how potential misinterpretations and out-of-context information are deployed.[194]

4. Analytical Tools and Databases

After CBP personnel collect social media information — including from ESTA and visa applications, from elec-

tronic devices searched under their claimed border search authority, and from numerous other sources[195] — the data is provided to analysts who conduct one or more of three main types of analyses:

A. **Assigning individual risk assessments:** comparing an individual's personally identifiable information against DHS-held sources to assess his or her level of risk, such as whether the individual or her associates may present a security threat, in order to determine what level of inspection she is required to undergo and whether to allow her to enter the country;

B. **Trend, pattern, and predictive analysis:** identifying patterns, anomalies, and subtle relationships in data to guide operational strategy or predict future outcomes;[196] and

C. **Link and network analysis:** identifying possible associations among data points, people, groups, entities, events, and investigations.[197]

These analytical capabilities are interrelated and interdependent and serve as the backbone of CBP intelligence work. Because the ways in which CBP conducts these analyses and draws conclusions from data depend heavily on interactions among the agency's various data systems, this section will provide an overview of the key systems and their analytical functions. It shows that the social media information in each of these databases is amassed on the basis of overbroad criteria and without accuracy requirements, shared widely with few or no restrictions, analyzed using opaque algorithms and tools, and often retained longer than the approved retention schedules.

A. Assigning Individual Risk Assessments

The primary system CBP uses for combining and analyzing data, including for assigning risk assessments, is the Automated Targeting System (ATS). There is scant publicly available information regarding the foundation, accuracy, or relevance of these risk assessments; nor do we know whether the factors used in assessments are non-discriminatory.[198] We do know, however, that social media is likely a common source in formulating risk assessments. ATS contains copies of numerous databases and data sets that include social media information, such as CBP's ESTA, the FBI's Terrorist Screening Database (TSDB), and data from electronic devices collected during CBP border searches.[199] ATS also appears to ingest social media information directly from commercial vendors.[200] CBP agents use secret analytic tools to combine the information gathered from these various sources, including from social media, to assign risk assessments to travelers, including Americans flying domestically.[201] These assessments may get a person placed on a watch list like the TSDB,[202] and determine whether the person gets a boarding pass or if additional screening is necessary.[203]

To be clear, the individuals who are subjected to these measures are not necessarily suspected of a crime or a link to criminal activity.[204] Rather, an individual's risk level is determined by a profile, which can be influenced by social media information contained in ATS or other databases, as well as ad hoc queries of information on the internet, including queries of social media platforms.[205] Notably, DHS exempted ATS from accuracy requirements under the Privacy Act, so the information that goes into one's risk assessment need not be correct, relevant, or complete.[206]

ATS's individual risk assessment capabilities are also leveraged by ICE in its enforcement activities against people who have overstayed their visas. ATS receives the names of potential overstays from CBP's arrivals and departures management system, and ATS automatically vets each name against its records to create a prioritized list based on individuals' "associated risk patterns."[207] The prioritized list is then sent to ICE's lead management system, LeadTrac (discussed further in the ICE Visa Overstay Enforcement section below).[208]

It is not clear what standard is used in determining "risk" in these profiles or how exactly social media information is weighted. But it seems likely that ATS's data mining toolkit, which includes "social network analysis" capabilities that may rely on social media information, is an important part of formulating risk assessments.[209]

Risk assessments and other records in ATS are retained for 15 years, unless the information is "linked to active law enforcement lookout records . . . or other defined sets of circumstances," in which case the information is retained for "the life of the law enforcement matter."[210] Notably, the most recent ATS privacy impact assessment admits that the system fails to "consistently follow source system retention periods, but instead relies on the ATS-specific retention period of 15 years," often retaining data for a period that exceeds the data retention requirements of the system from which it originated (for instance, three years for sources from ESTA).[211] Therefore, ATS passes information to partners long after it has been corrected or deleted from other databases.

ATS information, including personally identifiable information, is disseminated broadly within DHS and to other federal agencies, and many DHS officers have direct access to ATS.[212] It is unclear, however, whether risk assessments and the underlying social media data on which they are based may be disseminated beyond ATS.

B. Trend, Pattern, and Predictive Analysis

Essential to the process of assigning risk assessments are the CBP-formulated "rules," or "patterns" identified as "requiring additional scrutiny," that CBP personnel use to vet information in ATS in order to evaluate an individu-

al's risk level.[213] These patterns are based on trend analyses of suspicious activity and raw intelligence, as well as CBP officer experience and law enforcement cases.[214] In addition to assigning risk assessments, ATS is used as a vetting tool by both USCIS (for refugees and applicants for certain immigration benefits) and the Department of State (for visa applicants) and to analyze device data obtained at the border.[215] For each of these functions, CBP agents use ATS to compare incoming information against ATS holdings and apply ATS's analytic and machine learning tools to recognize trends and patterns.[216]

CBP agents also use ATS for preflight screenings (which will be discussed in more detail in the TSA section) to identify individuals who, though not on any watch list, "exhibit high risk indicators or travel patterns."[217] ATS's analytic capabilities likely underpin its determinations of "high risk" patterns.

ATS is also central to a DHS-wide "big data" effort, the DHS Data Framework. Similar to ATS in structure and purpose but wider in scope, the Data Framework is an information technology system with various analytic capabilities, including tools to create maps and time lines and analyze trends and patterns.[218]

The Data Framework ingests and analyzes huge amounts of data from across the department and from other agencies.[219] Originally the Data Framework was meant to import data sets directly from dozens of source systems and categorize the data in order to abide by retention limits, access restriction policies, and ensure that only particular data sets are subject to certain analytical processes.[220] However, as of April 2015, data sets started being pulled straight from ATS instead of from the source systems, and the Data Framework stopped tagging and categorizing data before running analytics.[221] DHS said this change was merely an "interim process" of mass data transfer in order to expedite its ability to identify individuals "supporting the terrorist activities" in the Middle East.[222] The interim process was originally established to last for 180 days, with the possibility of extensions in 90-day increments.[223] However, the interim period continued for at least three and a half years (April 2015–October 2018), and it is unclear whether it is still ongoing.[224]

The Data Framework's interim process and its extraction of data directly from ATS are troubling in part because ATS does not comply with the retention schedules of different source systems but rather tends to rely on its own 15-year retention period.[225] By bypassing source systems and extracting information directly from ATS, the interim process creates a risk that outdated or incorrect information, or information that was deleted from its source system many years earlier, will be input into the Data Framework's classified repository. Hence, information collected from an individual for one purpose — such as screening for the Visa Waiver Program — not only is retained longer than it should be, but is channeled into larger and larger analytical systems for unknown and unrelated purposes.

According to DHS senior leadership, the Data Framework also incorporates "tone" analysis.[226] Purveyors of tone analysis software have made dubious claims about its ability to predict emotional states and aspects of people's personality on the basis of social media data.[227] These claims, however, have been thoroughly debunked by empirical studies.[228] The unreliability of such software increases dramatically for non-English content, especially when people use slang or shorthand, which is often the case with social media interactions.[229]

The Data Framework and its analytical results are used extensively throughout DHS, including by CBP, DHS's Office of Intelligence and Analysis, TSA's Office of Intelligence and Analysis, and the DHS Counterintelligence Mission Center.[230] DHS uses the Data Framework's classified data repository to disseminate information externally, including "bulk information sharing" with U.S. government partners.[231]

C. Link and Network Analysis

A central element of CBP network analysis capabilities is the collection of information on a huge number of individuals in order to draw connections among people, organizations, and data. For this purpose, CBP agents use the CBP Intelligence Records System (CIRS) to gather information about a wide variety of individuals, including many who are not suspected of any criminal activity or seeking any type of immigration benefit, such as people who report suspicious activities; individuals appearing in U.S. visa, border, immigration, and naturalization benefit data who could be associates of people seeking visas or naturalization, including Americans; and individuals identified in public news reports.[232] The system stores a broad range of information, including raw intelligence collected by CBP's Office of Intelligence, data collected by CBP pursuant to its immigration and customs authorities (e.g., processing foreign nationals and cargo at U.S. ports of entry), commercial data, and information from public sources such as social media, news media outlets, and the internet.[233] Notably, the system is exempt from a number of requirements of the Privacy Act that aim to ensure the accuracy of records.[234] Accordingly, it appears that information in CIRS may be ingested, stored, and shared regardless of whether it is accurate, complete, relevant, or necessary for an investigation. There is no public guidance on quality controls for information eligible for inclusion in CIRS.[235]

Huge swaths of data from CIRS, ATS, and other systems, including social media information, are then ingested by another database, the Analytical Framework for Intelligence (AFI).[236] AFI provides a range of analytical tools that allow DHS to conduct network analysis, such as identifying links or "non-obvious relationships" between individuals or entities based on addresses, travel-related information, Social Security numbers, or other information, including social media data.[237]

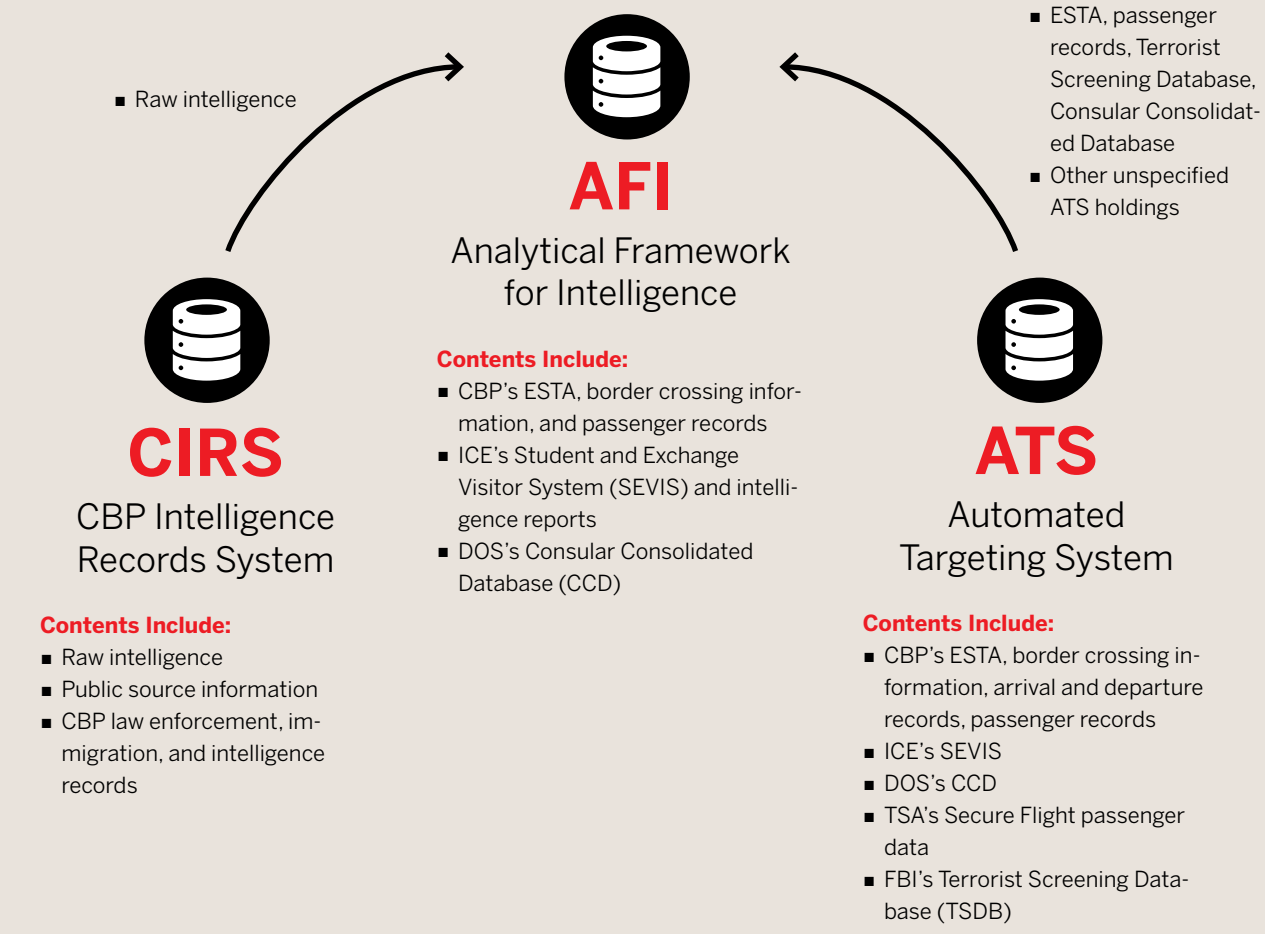
It is possible that ATS risk assessments are among the

unspecified data transferred from ATS to AFI.[238] In addition, AFI users may upload internet sources and other public and commercial data, such as social media, on an ad hoc basis.[239] The data need only be relevant, a fairly low standard, and the rules allow data of "unclear" accuracy to be uploaded.[240] CBP agents use AFI to search and analyze databases from various sources, including Department of State and FBI databases and commercial data aggregators.[241] Social media information in AFI can be used in ongoing projects and finished intelligence products, which can be disseminated broadly within DHS and to external partners.[242]

The data mining firm Palantir — a longtime government contracting partner that helped facilitate one of the National Security Agency's most sweeping surveillance programs[243] — is intimately involved in AFI's operation.[244] Documents obtained by the Electronic Privacy Information Center (EPIC) through a Freedom of Information Act (FOIA) request refer to joint "AFI and Palantir data" and state that "data from AFI and Palantir can be shared with other stakeholder[s] and agencies" in compliance with AFI rules.[245] "Palantir data" may refer to personal information about people that Palantir ingests from disparate sources—such as airline reservations, cell phone records, financial documents, and social media — and combines into a colorful graphic that purports to show software-generated linkages between crimes and people.[246]

According to an investigation by Bloomberg News, law enforcement agencies may use this "digital dragnet" to identify people who are only very tangentially related to criminal activity: "People and objects pop up on the Palantir screen inside boxes connected to other boxes by radiating lines labeled with the relationship: 'Colleague of,' 'Lives with,' 'Operator of [cell number],' 'Owner of [vehicle],' 'Sibling of,' even 'Lover of.'"[247] The value of discovering such linkages in investigations, while much hyped, is open to debate.[248] And as the volume of information grows, so does the risk of error. Given that the information in AFI is not required to be accurate, it is likely that the data from Palantir is similarly unverified.[249] Palantir also supplies AFI's analytical platform

Data Transfer From CIRS & ATS to AFI



and works extensively with ICE, as discussed later.[250]

Since 2015, CBP has awarded contracts worth about $3.2 million to Babel Street, an open-source and social media intelligence company, for software licenses and maintenance for the CBP unit that manages AFI, the Targeting and Analysis Systems Program Directorate.[251] According to the company's website, Babel Street technologies provide access to millions of data sources in more than 200 languages; a number of analytic capabilities, including sentiment analysis in 18 languages; and link analysis.[252] Users can also export data to integrate with Palantir analytic software.[253] CBP likely uses Babel Street's web-based application, Babel X, which is a multilingual text-analytics platform that has access to more than 25 social media sites, including Facebook, Instagram, and Twitter.[254] There are few details about how Babel Street software is used by CBP and what sorts of social media data it may provide for AFI.

Additionally, ATS and the DHS Data Framework both have their own link and "social network" analysis capabilities, though little is known about how those capabilities function.[255]

In sum, while we know that CBP undertakes extensive analyses of social media information, from assessing risk level to predictive and trend analysis to "social network analysis," we know almost nothing about the validity of these techniques or whether they are using discriminatory proxies. Partnerships with data mining companies such as Palantir raise additional concerns about the incorporation of large pools of unverified data into DHS systems, as well as privacy concerns about allowing a private company access to sensitive personal data.[256] The increasing consolidation of data into CBP's expansive intelligence-gathering databases, as well as into the DHS Data Framework, further compounds the issues created by DHS's vague, overbroad, and opaque standards for collection of social media data and its tendency to recycle that data for unknown and potentially discriminatory ends.

Transportation Security Administration

The Transportation Security Administration (TSA) is in charge of security for all modes of transportation — aviation, maritime, mass transit, highway and motor carrier, freight rail, and pipeline — into, out of, and within the United States.[257] Although most visible at airports, TSA also works behind the scenes via its Secure Flight program, which runs passenger records against a variety of watch lists and information held in CBP's Automated Targeting System (ATS).[258] As with ATS's risk assessments, very little is publicly known about the scientific foundation and validity of TSA's security determinations. We do know that many of the lists that TSA uses to vet passengers rely on social media information, with the attendant risks of misinterpretation, and have been widely criticized for being inaccurate.[259]

Concerns about TSA's use of social media information are compounded by the lack of transparency surrounding how individuals are designated as security risks.

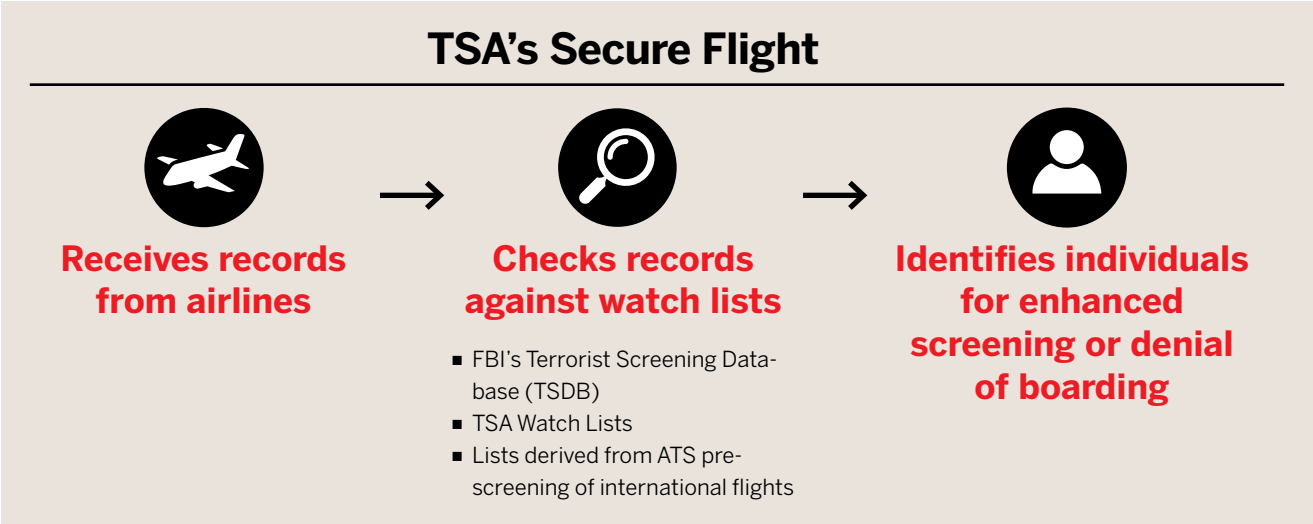
TSA's Secure Flight program collects passenger records from airlines and works in conjunction with CBP's ATS to flag passengers for enhanced screening or denial of boarding.[260] Secure Flight checks roughly two million passenger records daily against a variety of watch lists.[261] Its automated matching system assigns a percentage score to each record, indicating the confidence level of a match between the passenger and a watch list entry.[262] Those whose scores meet the minimum threshold are identified and subjected to enhanced security screening by on-the-ground TSA personnel.[263] Secure Flight also identifies a (potentially overlapping) category of travelers and their companions called "Inhibited Passengers," which includes individuals who are confirmed or possible matches to watch lists, as well as individuals about whom DHS possesses "certain derogatory holdings that warrant enhanced scrutiny" or who have "a high probability of being denied boarding."[264] Both of the latter categories remain undefined.

The watch lists used to designate individuals as security risks include the No Fly and Selectee components of the Terrorist Screening Database (TSDB), TSA Watch Lists, and watch lists derived from ATS's prescreening of international flights.[265] Social media forms part of the basis for placing individuals on these watch lists, which are described below.[266]

1. Watch Lists

A. Terrorist Screening Database

Maintained by the FBI's Terrorist Screening Center and commonly known as the "terrorist watch list," the TSDB is the database of individuals whom the government categorizes as being "known" or "suspected" of having ties to terrorism.[267] DHS receives information from the TSDB through the DHS Watchlist Service, which main-



tains a synchronized copy of the database and disseminates records from it to parts of DHS.[268] The FBI and other federal agencies submitting nominations for the TSDB are encouraged to include social media information as a source for suspicion, even if the information is uncorroborated.[269] The watch list has long been criticized for being bloated and error prone; as of 2016 it included one million names, including those of about 5,000 Americans.[270] The standards for categorizing individuals as "suspected" of ties to terrorism are so broad that even people three degrees removed from a "suspicious" person could be included on the list.[271]

The TSDB is the source of the No Fly List and the Selectee List, both of which also rely on broad standards that could allow, for example, the inclusion of individuals who have engaged in civil disobedience.[272] The No Fly List has been the subject of extensive litigation, in which federal courts have criticized the government's failure to ensure adequate procedures to allow individuals to contest their inclusion on the list.[273]

B. TSA Watch Lists

The watch lists created and managed by TSA's Office of Intelligence and Analysis are also likely to incorporate social media information in at least some cases.[274] These lists are based on information in TSA Intelligence Service Operations Files, which are compiled from TSA security incidents, intelligence provided by other agencies, and broadly from commercial sources and publicly available data; they are used to flag people who are not on another relevant watch list to receive additional scrutiny during travel.[275] One such list, the "95 list," created in February 2018, includes individuals who make physical contact with a TSA employee or dog, loiter near screening checkpoints, are the subject of a credible threat of violence, or are "publicly notorious."[276] While some of this information likely comes from agents, it seems that public notoriety and perhaps even the threat of violence are factors that TSA gleans from social media.

C. ATS-Generated Watch Lists

TSA's Secure Flight also screens passenger records against watch lists derived from ATS's prescreening of international flights.[277] The ATS prescreening is informed by TSA-crafted rules or "threat-based intelligence scenarios," which ATS then compares against both passenger records and its plethora of other sources, including social media. ATS identifies individuals for enhanced TSA screening based on "matches" to information found in ATS.[278] Such matches could be based on a profiling rule or based on a passenger's identifiers, which may include names, phone numbers, or social media handles.[279] ATS compiles its list of matches to share with Secure Flight, including individuals who, though not on any other watch list, "exhibit high risk indicators or travel patterns."[280] There are no public criteria for what constitutes a high risk indicator or travel pattern that could trigger a flag on ATS.

According to a privacy impact assessment published in April 2019, TSA uses ATS to generate watch lists for

International Flight Data Transfer

Airlines →

- Share passenger records with Secure Flight

Secure Flight →

- Shares passenger records for international flights, overflights, and point-to-point flights with CBP's ATS
- Also shares information on TSA-identified "Inhibited Passengers" with ATS

CBP's ATS →

- Performs prescreening:
  1. Applies TSA-crafted "threat-based intelligence scenarios," ATS "risk-based rules," and federated queries
  2. From prescreening, creates watch list of international passengers to share with TSA's Secure Flight
- Shares CBP-held information on "Inhibited Passengers" with Secure Flight

Secure Flight

- Based on ATS prescreenings of international flights, determines whether passengers on ATS-derived watch lists and "Inhibited Passengers" are to be subjected to enhanced screening or denial of boarding

TSA's "Silent Partner" and "Quiet Skies" programs.[281] Little is known about Silent Partner, but according to internal TSA documents, Quiet Skies originally involved undercover federal air marshals shadowing thousands of travelers on flights and through airports, documenting whether travelers use a phone, go to the bathroom, fidget, or have a "cold penetrating stare," among other behaviors.[282] Following a series of reports by the *Boston Globe,* TSA announced that it curtailed the Quiet Skies program in December 2018 and will no longer require agents to compile reports on travelers who exhibit routine passenger behaviors.[283] However, TSA now uses ATS, with its numerous social media sources, to create a list of travelers for Quiet Skies. TSA formulates rules for CBP personnel to check against ATS holdings on passengers on outbound international flights and domestic flights subsequent to international flights to create a Quiet Skies List of individuals designated for enhanced screening.[284] A similar Silent Partner List is created for passengers on in-bound international flights.[285] In addition to being designated for enhanced screening, individuals on the Quiet Skies and Silent Partner Lists may be subject to "observation by the TSA Federal Air Marshal Service (FAMS) while the individual is onboard the flight or in the airport."[286]

The privacy impact assessment notes that individuals "will remain on the Quiet Skies List for a period of time," though the period is unspecified.[287] Names of individuals who are flagged in ATS based on matches to TSA's rules are retained in ATS for seven years, while names of international travelers whose activities do not match the risk patterns are retained for seven days "to conduct additional analysis."[288] This information can be used for future risk assessments and watch lists.[289]

Social media also plays a role in TSA screenings of passengers on domestic flights.[290] For domestic flights, Secure Flight screens airline records using watch lists and unspecified "rules" and then shares the names of watch list matches and other "Inhibited Passengers" with ATS.[291] ATS users then perform comparisons, apply "risk-based rules," and conduct federated queries to identify pertinent CBP-held information on those travelers, which could include social media information. At the same time, ATS users create a separate list of CBP-identified "Inhibited Passengers" based on analyses of ATS sources, including social media.[292] CBP sends the results of the ATS screening back to Secure Flight, and TSA and CBP personnel compare the Secure Flight and ATS-generated lists of "Inhibited Passengers" via a common dashboard display.[293] TSA agents then make final decisions on enhanced screening and boarding denial, which could be informed by the ATS-held social media records.[294]

Additionally, TSA agents use an ATS "decision-support" tool called ATS-Passenger (ATS-P), available on mobile devices through an ATS mobile application, to view information in ATS and create a prioritized list of "potentially high-risk passengers."[295] According to the most recent privacy impact assessment, TSA personnel can search and filter ATS information by creating "user-defined rules" based on "operational, tactical, intelligence, or local enforcement efforts."[296] The ability of each user to define his or her own rules — a process about which there is little information publicly available — creates opportunities for discriminatory application. ATS-P also allows users to query other available federal government systems and publicly available information, including social media data.[297] The fact that this system is applied to domestic flights raises the possibility that it could be used to target American travelers on the basis of their political and religious views.

Domestic Flight Data Transfer

Airlines →

- Share passenger records with Secure Flight

Secure Flight →

- Screens passenger records against watch lists and unspecified "rules"; identifies " Inhibited Passengers"
- Shares information on TSA-identified "Inhibited Passengers" with CBP's ATS

CBP's ATS →

- Performs comparisons, applies "risk-based rules," and conducts federated queries
- Shares CBP-held information on CBP- and TSA-identified "Inhibited Passengers" with Secure Flight

Secure Flight

- Determines whether passengers are to be subjected to enhanced screening or denial of boarding

2. TSA PreCheck

TSA also uses Secure Flight to identify low-risk passengers for TSA PreCheck, a fee-based program that allows travelers expedited transit through airports.[298] Secure Flight screens PreCheck applicants against its own information as well as several lists of preapproved low-risk travelers from other agencies and other parts of DHS, including CBP's Trusted Traveler programs.[299] Since these lists rely on databases that include social media information, it is likely that what people say on social media influences PreCheck designations.[300]

Indeed, TSA has sought to highlight social media in its PreCheck screening efforts. In December 2014, the agency announced that it was planning to expand PreCheck by hiring contractors to screen applicants using "risk scoring algorithms using commercial data, including social media and purchase information."[301] In response to criticism from civil society about the use of social media data and the reliance on private companies to determine security risks,[302] TSA backtracked, issuing a revised proposal that barred bidders from using any available social media for prescreening efforts.[303] In September 2017, TSA awarded an ongoing contract worth more than $22 million to Idemia, a big-data biometrics company, for Universal Enrollment Services, which includes PreCheck enrollment.[304] Idemia captures and submits enrollment data, including biographic, biometric, identity, and citizenship documentation, to the government for vetting and case management purposes.[305] While the contract documents do not indicate that Idemia will use social media information to conduct "security threat assessments" and "identity assurances" for PreCheck, Idemia's website describes the company's data mining mission in general as including "geolocations, audit trails and social media conversations."[306]

In sum, TSA's Secure Flight uses a range of watch lists that rely at least in part on social media information in its preflight screening and decision making, about which very little is known. TSA and CBP also have an extensive information-sharing arrangement in which TSA relies on ATS holdings, which include social media data, to screen "Inhibited Passengers" and to aid in "decision-support" via the ATS mobile application. TSA's PreCheck also may include the collection and analysis of social media information to designate certain individuals as "low risk." The use of context-dependent and easily misinterpreted social media in secret analyses raises concerns about the use of discriminatory criteria to target travelers, both domestic and international, as well as the impact on free speech.

U.S. Immigration and Customs Enforcement

Immigration and Customs Enforcement (ICE) investigates cross-border crime and immigration violations.[307] Its activities range from combating child pornography and human trafficking to conducting raids at workplaces and targeting people, including activists, for immigration violations outside courthouses and schools.[308] ICE relies on social media data, which is often unreliable, to support its extremely broad investigative authorities; the agency has also explored expanding its collection of social media data to make dubious and likely discriminatory judgments about whether individuals should be permitted to enter or remain in the country.

ICE has two main branches: Homeland Security Investigations (HSI), which conducts both criminal and civil investigations, and Enforcement and Removal Operations (ERO), which is primarily responsible for detention and deportation.[309] Most of the activities described below are conducted by HSI — the second-largest investigative arm in the federal government[310] — which extracts, consults, and analyzes social media data during its investigations, including vetting and investigating overstay leads and conducting warrantless border searches, as well as in its intelligence-gathering and analysis initiatives. In turn, these investigations inform ERO's removal operations.

1. Investigations

HSI often relies on social media in conducting an investigation.[311] First, ICE agents may manually collect data from publicly available and commercial sources, including social media, whenever they determine that the information is "relevant for developing a viable case" and "supports the investigative process."[312] According to privacy impact assessments, such information is meant to be used to verify information that is already in the agency's possession, such as a target's current and former places of residence and cohabitants, and to identify other personal property.[313] However, it may also be used "to enhance existing case information" by providing identifying details like date of birth, criminal history, and business registration records.[314]

Social media information is also gathered during undercover operations related to criminal investigations, during which agents are permitted to "friend" individuals on social media sites and collect any information they come across as a result.[315] In addition, HSI agents gain access to social media information through other investigatory activities — namely vetting and overstay enforcement initiatives and extractions of data from electronic devices obtained during border searches and investigations — which are discussed in the next sections.

The Investigative Case Management (ICM) system is the primary database that stores information collected by ICE during criminal and civil investigations.[316] ICE agents can use ICM to automatically query a plethora of internal and external systems, as well as to manually search various pools of data and copy and upload the results; the information ICE can query includes results from CBP's Automated Targeting System (ATS), which contains social media information from a number of sources.[317] ICM data is disseminated within DHS and shared broadly with outside agencies.[318] In addition to wide authority to share information through formal channels with state, local, and federal law enforcement agencies, ICE agents are known to share information informally with individual state or local law enforcement officers.[319] In addition, ICM records that pertain to individuals, or "subject records," are shared via the Law Enforcement Information Sharing (LEIS) Service, a web-based data exchange platform that allows partner law enforcement agencies to access DHS systems, including but not limited to ICM and TECS, CBP's primary law enforcement system.[320]

ICM was developed by the private data mining company Palantir.[321] According to contract notices, Palantir currently has a contract for work relating to ICM that has so far totaled $51.6 million.[322] Though Palantir's 2014 proposal for ICM described the system as intended for use by ICE's investigative branch, HSI, in 2016 DHS disclosed that it is also used by ICE's deportation branch, ERO, to obtain information "to support its civil immigration enforcement cases."[323]

ICE has also invested in other software systems to enable it to analyze information from social media. For example, in June 2018, it was reported that ICE had signed a $2.4 million contract with Pen-Link,[324] a company offering software to law enforcement that can collect and analyze "massive amounts of social media and internet communications data."[325] One of the services included in the Pen-Link contract with ICE is Pen-Link X-Net,[326] which collects and analyzes large quantities of internet-based communications data, from an "extensive, ever-growing list of providers," including social media platforms.[327] Such sweeping collection and analysis is likely to scoop up swaths of irrel-

evant and unreliable information and risks misinterpreting innocuous connections and patterns as illicit activity.

Finally, West Publishing, a subsidiary of Thomson Reuters, provides HSI with access to the company's Consolidated Lead Evaluation and Reporting (CLEAR) system, through a 2017 contract worth $20 million.[328] CLEAR combines a wide array of public and proprietary records, including data from social networks and chat rooms, to create "customizable reports, Web Analytics, mapping, and link charts."[329] According to other contract documents, CLEAR provides essential support to ICE's ability to investigate criminals and to uphold and enforce customs and immigration law "at and beyond our nation's borders."[330] CLEAR also interfaces with information from Palantir as well as with ICE's main analytical system, FALCON.[331]

2. Visa Overstay Enforcement

ICE has identified visa overstays as a serious threat to national security and over the past several years has ramped up its enforcement, tracking travelers who have allegedly remained in the United States beyond the time originally permitted; its efforts have included social media monitoring.[332] While two of the 9/11 hijackers had overstayed their visas,[333] there is little evidence that overstays pose a significant ongoing threat to national security. Research from the Cato Institute shows that the chance of being killed in an attack by a foreign-born terrorist is 1 in 4.1 million for an attacker on a tourist visa and 1 in 73 million for an attacker on a student visa, the two most common overstay categories.[334] Given that the overstay rate in 2017 was 2.06 percent for tourist visas and 4.15 percent for student visas, the chance of being killed by someone overstaying a visa is infinitesimal.[335]

At a May 2017 congressional hearing, DHS described the basic process used to vet overstay leads: CBP's arrivals and departures management system sends potential leads — identified by matching entry and exit records — to ATS, which automatically screens, prioritizes, and sends them over to ICE's lead management system, LeadTrac.[336] Analysts then vet these leads — against government databases, public indices, and unnamed commercial databases that provide aggregated information from social media and other public sites, as well as through internet searches on social media platforms — to determine whether there is a potential violation that could require a field investigation.[337] According to DHS documents prepared for the incoming administration at the end of 2016, ICE personnel target individuals for overstay enforcement who exhibit "specific risk factors," which are based in part on "analysis of dynamic social networks."[338] These analyses of social networks may be informed by the data gathered from social media sites. According to the DHS inspector general, ICE agents do not have policies and guidance on "appropriate system use" of the roughly 17 information technology systems upon which analysts rely for overstay work.[339]

In 2014 ICE set up a special unit called the Open-Source Team, which uses a broad range of publicly available information, including social media, to help "locate specific targeted individuals, identify trends and patterns, and identify subtle relationships."[340] A document obtained by the Brennan Center via FOIA request highlights three Open-Source Team "success stories," all of which involve individuals from Muslim-majority countries.[341]

In August 2016, ICE launched a series of pilot programs that aim to use social media to bolster vetting, lead investigation, and enforcement.[342] One of these programs, the "Domestic Mantis Initiative," vets leads pulled from the Student and Exchange Visitor System (SEVIS) on students who enter the United States planning to study a "nonsensitive" field of study and later change to one the State Department categorizes as "sensitive" because of its potential connection to national security–related technology (e.g., nuclear physics, biomedical engineering, and robotics).[343] Using social media and other sources, ICE continuously monitors these students during their time in the United States, although it is not known what would constitute suspicious activity that would cause immigration authorities to take action.[344]

Also in August 2016, ICE launched another pilot program, most often referred to as the Overstay Lifecycle program.[345] According to a report by the DHS inspector general, the program screens the social media activity of a category of nonimmigrant visa applicants from certain countries to help uncover "potential derogatory information not found in Government databases"; both the category of applicants and the specific countries involved were redacted from the publicly available report.[346] The report noted that the pilot was to screen social media activity at the time of visa application and to "continue social media monitoring" (during a time frame or process that was redacted from the report, but could extend to the time that subjects were in the United States) using a "web search tool" that analyzes social media data to develop so-called "actionable information."[347] As with other uses of social media by DHS, it is unclear what types of information would raise flags about visa applicants.

ICE's Overstay Lifecycle program was designed to supplement PATRIOT, an existing program that screened applicants at 28 visa security posts but did not monitor people who were granted visas and traveled to the United States.[348] The newer program aims to close this gap in enforcement by conducting continuous vetting and monitoring of some visa applicants, from the time they file a visa application to the time they depart from the country or violate their terms of admission, to uncover any "derogatory information."[349]

The visa applicants subject to continuous monitoring would be those who have applied through one of "at least two" specific State Department posts abroad, though the posts are not publicly identified.[350] According to the 2016

DHS report to Congress, these posts would be selected "to complement existing HSI screening efforts and in response to recent global acts of terrorism perpetrated in those countries."[351] According to the same report, DHS also planned to incorporate social media vetting tools into both PATRIOT and LeadTrac, and modify LeadTrac to ingest information from visa applicants upon entry.[352] It is not clear whether this system change has occurred.

It is clear, however, that ICE has relied heavily on the data mining firm Giant Oak, Inc., to support these programs and will continue to do so in the future. According to publicly available contract notices, in August and September of 2018, both ICE's Visa Security Program and its Counterterrorism and Criminal Exploitation Unit (CTCEU) contracted with Giant Oak for "open source/social media data analytics."[353] These contracts are in addition to previous social media data analytics contracts between ICE and Giant Oak.[354] A contract recently obtained by the Brennan Center via FOIA request shows that CTCEU utilizes Giant Oak's Search Technology tool (GOST) to aid in proactive investigation of national security leads that have incomplete address information or were returned from field investigations unresolved.[355] This tool is used for bulk screening and prioritization of individuals based on "threat level" and continuously monitors and evaluates changes in patterns of behavior over time. According to the CEO of Giant Oak, the tool lets the government know when overall patterns change—for example, when a group of individuals becomes "more . . . prone to violence."[356]

According to the contract, Giant Oak continuously monitors social media and other online sources and returns to CTCEU any information that identifies an individual's possible location (including location of affiliated organizations), contact information, and employers.[357] Upon "exhaustion" of that so-called tier 1 information, ICE can request a follow-up search for information about the person's associates (e.g., friends, family members, coworkers) that could help locate an individual.[358] The documents also note that the contract grants a Giant Oak "Social Scientist" access to classified information; he/she "tweaks the algorithms" behind GOST to better serve CTCEU's needs, and works to further specialize the transliteration and name matching tools for "certain ethnic groups, non-Roman languages and alphabets, or countries of origin."[359] There is no publicly available information on the scope of ICE's other contracts with Giant Oak.

3. Extreme Vetting

As detailed below, after sustained opposition from many stakeholders, ICE announced in May 2018 that it had shelved its search for an automated tool for its Extreme

Automated Extreme Vetting

ICE's proposal for an automated Extreme Vetting Initiative neatly illustrates many of the problems raised by social media monitoring.[i] The initiative was based on the first Muslim ban ordered by President Trump, which called for the development of a vetting tool to examine whether an individual coming to the United States would be "a positively contributing member of society," "make contributions to the national interest," or commit a crime or terrorist act.[ii] Although the order was enjoined by federal courts as motivated by animus toward Muslims, ICE wanted to find out if a company could build software to monitor the online universe to determine whether would-be travelers met these criteria.[iii] The proposed venture raised several concerns:

>> **As a group of 54** machine-learning experts wrote to the DHS secretary, no algorithm can make judgments about such subjective matters as who will make a positive contribution to society or the national interest.[iv] Its developers would have to use proxies that are unscientific and reflect biases and unfounded assumptions. A Facebook post criticizing U.S. foreign policy, for example, could be tagged as a threat to national security.

>> **A computer also cannot** predict in any reliable way if a person intends to commit a terrorist act or other crime. Given the size of the U.S. population and immigration rates, crime is rare and terrorism even more so, and even the best algorithms make too many mistakes when predicting rare events.[v]

>> **Subjective standards,** such as whether someone would be a "positively contributing member of society," open the door to discrimination, a risk amplified by the origin of the program in the Muslim ban. As the Congressional Black Caucus observed, "[D]riven by a discriminatory agenda, ICE is trying to give itself maximal latitude to monitor and deport whomever it wants, whenever it wants."[vi]

>> **Social media accounts** are difficult to verify, and messages are notoriously hard to interpret. Cultural and linguistic differences, standard in immigration processes, amplify these problems.

>> **People censor themselves** when they know the government is watching. Although the initiative was directed at foreigners, it would inevitably scoop up information from people living in the United States, such as their family members and associates — and even noncitizens living in the United States have constitutionally protected rights.

In May 2018, ICE backed down from the automated component of the initiative, acknowledging that no software could make the types of predictions it was seeking.[vii]

Vetting Initiative (now rebranded as the Visa Lifecycle Vetting Initiative).[360] Instead, it has opted to spend $100 million to hire "roughly 180 people to monitor the social media posts of those 10,000 foreign visitors flagged as high-risk, generating new leads as they keep tabs on their social media use."[361] Monitoring will continue while these individuals are in the United States, although ICE has stated that it would stop if a visitor was granted legal residency.[362] There is no public information on the types of social media posts that ICE considers indicative of risk, but if ICE endeavors to undertake predictive tasks based on the criteria outlined in the first version of this program, there is a high risk that the program can be used in discriminatory ways.

ICE awarded this reimagined, human-centered monitoring contract to SRA International (now CSRA Inc., owned by General Dynamics) in June 2018; several vendors filed challenges, which were ultimately denied by the U.S. Government Accountability Office (GAO).[363] As of the publication of this report, no funds had yet been awarded to SRA to carry out the contract.[364]

As the above discussion makes clear, ICE relies heavily on social media to vet certain categories of individuals at the time of application. It is likely that these are predominantly individuals who are the focus of the Trump administration's anti-Muslim extreme vetting initiatives. Moreover, the agency is moving toward using social media to monitor and track visa holders and students throughout their stay in the United States, where they would be covered by the First Amendment. It is also evident that the agency intends to rely more and more on software and other automated technologies, which the USCIS pilot programs, discussed earlier, determined were of limited usefulness.[365]

Finally, it is worth highlighting that many of the ICE programs described above have been rolled out as pilots. While pilot programs are a useful way to assess new tools, ICE does not seem to systematically measure their effectiveness. It also does not issue privacy impact assessments for most of these activities, which would at least provide a bare minimum of information to illuminate the impacts of ICE programs. Last, public information provided by ICE does not clearly indicate which pilots are still active and how they relate to newer initiatives, leaving the public in the dark about the agency's activities.

4. Electronic Device Searches

ICE also collects, extracts, and analyzes information, including social media data, from electronic devices (e.g., cell phones, laptops, tablets, thumb drives) obtained during warrantless border searches and investigations pursuant to search warrant, subpoena, or summons, or provided voluntarily.[366] For the past decade, ICE, like CBP, has invested in Cellebrite Universal Forensic Extraction Devices (UFEDs), hand-held tools that can instantly extract the full contents of any device, including phones, laptops, and hard drives.[367] In recent years ICE has ramped up its purchasing of UFEDs, spending an additional $3.7 million on the tools (which cost between $5,000 and $15,000 each) and licensing since March 2017.[368] Though it is not known precisely in what circumstances and for what purposes ICE personnel use these devices, it is clear that ICE has the capability to easily extract swaths of data, including social media information, from electronic devices. While the searches of devices obtained during investigations are limited by the scope of the relevant search warrant, subpoena, or summons, ICE claims virtually unchecked authority to search and extract data from devices seized at the border, including social media data and other personal information.

A. Warrantless Border Searches

ICE, like CBP, collects information obtained from electronic devices at the border, which it justifies as necessary to supplement its investigations and enforcement of immigration laws.[369] Whereas CBP recently issued a revised policy on its border searches, ICE operates under policy guidance issued nearly a decade ago. This guidance includes neither the stricter rules for forensic searches nor the restrictions on accessing data stored in the cloud or remote networks that CBP added to its guidance seemingly in response to a federal court case.[370] Instead, it allows agents to "search, detain, seize, retain, and share" electronic devices and any information they contain without individualized suspicion.[371] In other words, ICE appears to claim a right of access to the full gamut of information on travelers' phones and in their social media accounts, even where there is no suspicion of wrongdoing.[372]

ICE claims its authority to search electronic devices at the border derives from statutes passed by the First Congress, such as the Act of August 4, 1790, which grants customs inspection authority over "goods, wares, or merchandise" entering the country.[373] Though the 2009 privacy impact assessment asserts that "travelers' electronic devices are equally subject to search" as the "merchandise" described in 1790, the amount of sensitive information contained in electronic devices like cell phones is hardly comparable.[374] Indeed, as the Supreme Court noted critically in a recent case, treating cell phones as functionally identical to other physical items of similar size "is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[375]

According to the relevant directive, detained devices are typically held for no more than 30 days, unless "circumstances exist that warrant more time."[376] Copies of the content obtained from devices are stored on either an ICE external hard drive or a computer system, neither of which is connected to a shared or remote network.[377] However, notes from any stage of the search process, typically relating to information that is "relevant" to immigration, customs,

or other laws enforced by DHS,[378] can be stored by ICE in "any of their recordkeeping systems," such as the Intelligence Records System.[379] The standard for relevance is left undefined, leaving ample room to collect a range of innocuous and often personal electronic content.

ICE can disseminate copies of information from an electronic device to federal, state, local, and foreign law enforcement agencies.[380] While ICE must have reasonable suspicion that the information on a device is evidence of a crime in order to share device information with other federal agencies for subject matter assistance, no suspicion is required to ask for technical assistance, which can encompass translation and decryption services.[381] Further, ICE is specifically authorized to disseminate any device information "relating to national security" to law enforcement and intelligence agencies.[382]

In short, ICE can access information stored on devices and from social media with no suspicion of criminal activity. It uses this information to support investigations and make admissibility determinations, but also as a broader means of information collection. There are few restrictions on how information obtained from electronic devices is used and disseminated. And the information, including social media identifiers and other personal data, can be stored in any number of ICE's databases, to which countless people have access, and shared with law enforcement as long as it is considered to "relate" to national security.

B. Extraction and Analysis of Electronic Media

Once ICE has obtained access to electronic devices through a warrantless border search or obtained access to "electronic media" (a slightly broader category that also includes thumb drives, hard drives, other storage devices, etc.) via subpoena[383] or warrant, it can extract and analyze information if the data could be "pertinent" to an investigation or enforcement activity.[384]

According to the 2015 Privacy Impact Assessment for the Forensic Analysis of Electronic Media, which encompasses electronic devices obtained during both border searches and investigations, the data extracted and analyzed by ICE could pertain to numerous individuals beyond the person in possession of the device, including witnesses, informants, members of the public, and victims of crimes.[385] Extracted data may also include sensitive personally identifiable information such as medical and financial information, records containing communications such as text messages and emails, and records of internet activity.[386] These records could reveal a host of sensitive data, including medical conditions, political and religious affiliations, and internet browsing preferences.

Information extracted from devices that are obtained during investigations is retained according to a proposed schedule that varies depending on the nature and outcome of the investigation.[387] There is extremely wide authority to disclose information to other agencies — including federal, state, local, and foreign law enforcement counterparts.[388] There also seems to be broad authority for re-dissemination by law enforcement partners.[389]

ICE uses a variety of unspecified electronic tools to analyze the media it extracts from devices via its border search authority or obtains during investigations.[390] The 2015 privacy impact assessment lists four types of analyses that agents can conduct using these tools: time frame analyses (to help determine when various activities occurred on a device), data hiding (to find and recover concealed data), application and file analyses (to correlate files to installed applications, examine a drive's file structure, or review metadata), and ownership and possession reviews (to identify individuals who created, modified, or accessed a given file).[391] The tools also can be used to "highlight anomalies" in the data.[392]

Social media information and other data extracted from electronic devices during investigations and border searches are stored in ICE's Intelligence Records System.[393] That data is then ingested into FALCON-SA, which has a number of analytical capabilities including "social network analysis," and will be discussed in the Analytical Tools and Databases section below.[394]

Thus, based on a low threshold of "pertinence," ICE uses sophisticated tools to extract social media data from electronic devices that it obtains during border searches and investigations. The extracted data is then subject to a variety of analyses (about which we know little), while notes about the information may be shared widely within and beyond DHS and potentially channeled into other systems for additional analyses. ICE's extraction of social media data from electronic media is yet another example of how the extensive DHS information-sharing apparatus enables data to be collected for one purpose under a malleable standard and then stored, shared, and reused for secondary purposes.

5. Analytical Tools and Databases

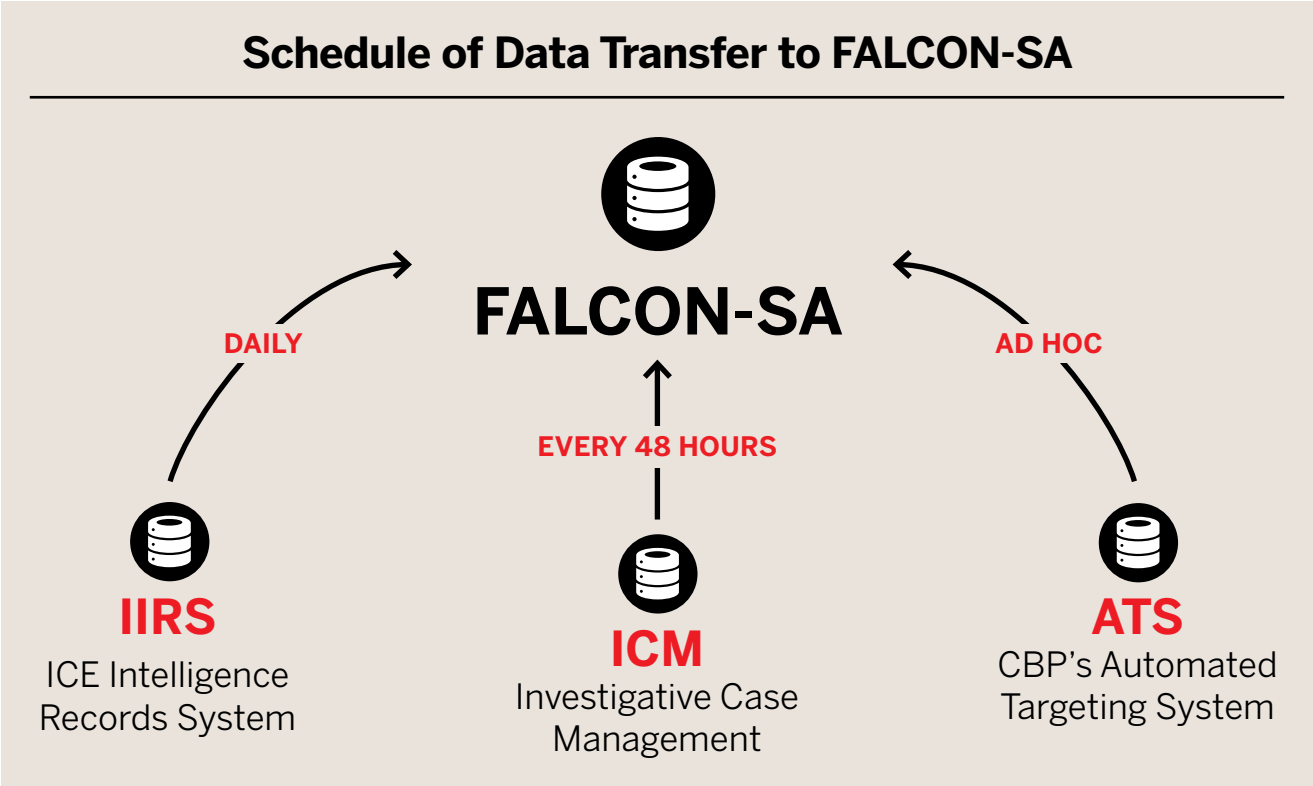
The numerous sources of information gathered by ICE operations and investigations are consolidated into several large databases. The main ICE database for compiling and analyzing social media information is the FALCON Search & Analysis System (FALCON-SA).[395] ICE personnel use FALCON-SA to conduct two kinds of analyses using social media data: trend analysis, or identifying patterns, anomalies, and shifts in data to guide operational strategy or predict future outcomes;[396] and link and network analysis, or identifying connections among individuals, groups, incidents, or activities.[397] This section will describe how FALCON-SA and its source systems enable these processes by gathering and storing information from numerous sources about a wide variety of individuals, disseminating information broadly, and applying unknown analytical tools to draw conclusions that impact ICE operations.

Although FALCON-SA does not itself extract data directly from social media, users can add social media information from other systems to FALCON-SA without restriction, and FALCON-SA automatically ingests data from several other databases that store social media information.[398] For instance, every day, FALCON-SA ingests information from ICE's Investigative Case Management (ICM) system relating to current or previous law enforcement investigations, as well as ICE and CBP lookout records,[399] which can include records of electronic devices searched at the border, including details gleaned from inspections of social media applications.[400] ICM also transfers to FALCON-SA telecommunications information about subjects of ICE criminal investigations, potential targets, associates of targets, or any individuals or entities who call or receive calls from these individuals.[401] On an ad hoc basis, ATS border crossing data and inbound/outbound shipment records are also uploaded into FALCON-SA.[402] While ICM's telecommunications data and ATS's border crossing and shipment data likely do not include social media information, once all these elements are combined with the other sources in FALCON-SA, the aggregation of information may collectively reveal a wealth of details about an individual's travels, family, religious affiliations, and more.[403]

FALCON-SA users are able to combine these various forms of information and apply the system's built-in trend analysis tools in order to highlight patterns, shifts in criminal tactics, emerging threats, and strategic goals and objectives.[404] These findings are then shared with DHS and ICE leadership, agents, officers, and other employees in the form of law enforcement intelligence products or reports. To produce these reports, FALCON-SA retains "all information that may aid in establishing patterns of unlawful activity," even if that information may not be strictly relevant or necessary for an investigation, and even if the accuracy of the information is unclear.[405]

To support its network analytics functions, FALCON-SA, like CBP's Analytical Framework for Intelligence, regularly ingests large amounts of information about individuals from another database, the ICE Intelligence Records System (IIRS).[406] IIRS, like the CBP Intelligence Records System, contains information on a wide variety of individuals, including people who are not suspected of any criminal activity or seeking any type of immigration benefit, such as associates of people seeking visas or naturalization, including Americans; people identified in public news reports; and people who have reported suspicious activities or incidents.[407] IIRS also contains electronic data and other information collected during ICE investigations and border searches, likely including social media data extracted from devices.[408] Sources for the system also include records from commercial vendors and publicly available data, such as social media information, which are not required to be relevant or necessary.[409]

Information from IIRS, ICM, and ATS is transferred to FALCON-SA, where it informs FALCON-SA's network analysis, highlighting associations between individuals and data elements.[410] Users can then identify possible connections among existing ICE investigations and create visualizations (e.g., maps, charts, tables) that display connections and



relationships among people and enterprises.[411] According to documents obtained by the Electronic Privacy Information Center via FOIA, FALCON has "social network analysis" capabilities that seem to rely on social media data.[412] ICE has not made clear whether ERO agents can directly access FALCON-SA to track down undocumented immigrants, although they can get such information from HSI.[413]

Notably, the operations of FALCON-SA, which is one of three ICE FALCON modules,[414] are intimately connected with ICE's contracts with the technology company Palantir.[415] According to the Palantir Licensing Terms and Conditions for FALCON, released in response to a FOIA request, FALCON is based on Palantir's Gotham platform, a software system unique to ICE that allows the agency to analyze complex data sets containing detailed personal information about individuals.[416] Publicly available contract notices reveal that in November 2018, Palantir began a new one-year, $42.3 million contract with ICE for "FALCON Operations & Maintenance," which brings the total for such contracts for FALCON to about $94 million.[417] Many aspects of Palantir's work with ICE — described in further detail in the Investigations section, above — remain undisclosed, such as the privacy protections for personal information, including social media data, that resides in FALCON-SA.

In sum, ICE's analytical tools aim to fully exploit the broad array of sensitive information, including social media data, collected by ICE agents and other DHS components. FALCON-SA houses social media data, for which there are no accuracy requirements, from numerous sources. This information is subjected to unspecified trend and network analyses, the efficacy of which is not publicly understood. While people seeking immigration benefits bear the brunt of this scrutiny, their American friends, relatives, and business associates are sucked into these repositories of information as well.

U.S. Citizenship and Immigration Services

U.S. Citizenship and Immigration Services (USCIS) processes and adjudicates applications and petitions for a variety of immigration benefits, including adjustment of status (for instance, from a student visa to a green card), naturalization, and asylum and refugee status.[418] USCIS's Fraud Detection and National Security Directorate (FDNS) performs background checks, processes immigration applications, investigates immigration benefit fraud, and functions as the link between USCIS and law enforcement and intelligence agencies.[419] The ambiguous nature of social media information collected by USCIS raises concerns about how it will be interpreted, especially for Muslims who are the targets of many of these programs. Indeed, while USCIS is expanding these programs, an inspector general report shows that the agency has not evaluated — much less demonstrated — their effectiveness.

1. Vetting

FDNS uses social media in a few contexts relating to its vetting initiatives, primarily to aid in determining an individual's admissibility or eligibility.[420] In 2014, FDNS started a pilot Social Media Division, which was made permanent in 2016. It was later expanded under an initiative known as FDNS "Enhanced Review."[421]

In 2015 and 2016, USCIS undertook five pilot programs to test the use of social media for screening and vetting. Four programs targeted refugees, and one focused on K-1 (fiancé[e]) visa applicants for adjustment of status.[422] While it is unclear which pilots have continued or been made permanent, public documents show that examining social media has become a key part of vetting refugees and asylum seekers in particular.

A. Vetting for Refugees and Asylum Seekers

According to DHS documents, the Social Media Division of FDNS performs social media vetting on "certain" asylum applications and screens refugee applicant data for "select populations" against publicly available information.[423] In October 2017, the director of USCIS told Congress that the "select populations" included Syrians, and that USCIS was working to refine and expand its use of social media to target additional categories of refugee and asylum applicants.[424] This statement came shortly after the Trump administration announced new "enhanced vetting capabilities" for refugees from 11 countries identified as posing a "higher risk."[425] The countries were not publicly identified by the administration, but it seems likely that this additional screening is targeted primarily at Muslims: the FDNS "Enhanced Review" was triggered by the Muslim ban executive order.[426] Refugee Council USA, a coalition of organizations focused on refugee protection and resettlement, told CNN that as of January 2018 the list of countries subject to enhanced review included Egypt, Iran, Iraq, Libya, Mali, North Korea, Somalia, South Sudan, Sudan, Syria, and Yemen.[427] Of the earlier social media pilots undertaken by USCIS, at least two focused solely on refugee applicants from Syria, one focused solely on refugee applicants from Syria and Iraq, and at least two used automated tools that were capable only of translating social media posts from Arabic.[428]

All refugee applicants, as well as those who gain status through an applicant (e.g., a spouse or child), undergo a variety of checks.[429] "Select applicant populations" are subject to social media checks, during which an FDNS officer looks at social media for information relating to their claim for refugee status or indication of potential fraud, criminal activity, or national security concerns.[430] During such checks, officers initially collect information using a government-affiliated account and username and do not interact with applicants through social media; this process is defined as overt research. When USCIS deems that an application presents a national security or public safety concern and overt research could "compromise the integrity" of an investigation, officers are permitted to use identities that do not identify their DHS or government affiliation in a process known as masked monitoring.[431]

A 2015 FDNS memorandum on the use of social media for refugee processing notes that officers will limit collection of information related to First Amendment–protected activities to information that is "reasonably related to adjudicative, investigative, or incident response matters."[432] The privacy impact assessment for refugee vetting notes that officers may provide the refuge seeker a chance to view and explain a social media posting found during vetting, and that the decision on a refugee's resettlement or employ-

ment eligibility cannot be made solely on the basis of information obtained from social media.[433]

As of November 2016, DHS reported that no immigration benefit had been denied "solely or primarily" as a result of information found on social media.[434] In fact, DHS concluded that information found during screening had merely a "limited" impact in "a small number of cases" in which the data was used for developing additional avenues of inquiry, and that social media information had little to no impact in the vast majority of cases.[435] This low "hit" rate raises questions about the value of focusing resources on collecting and analyzing this type of data.

For asylum seekers, DHS officers compare information from social media and other public and commercial sources against the information that applicants provide regarding when they entered the United States, how long they have been in the country, and even when they "encountered harm outside the United States."[436] Asylum officers are trained to compare public and commercial data with "applicant-reported information"; if they find an inconsistency, they "must confront the applicant with that information" and provide an opportunity to explain it.[437]

Although FDNS has tested automated tools to vet the social media of individuals seeking refuge, the extent to which such tools are currently used is not known. In pilot programs related to refugee applications, officers identified serious problems with the tools tested. Some of these were practical problems, such as language limitations (most tools are English-focused) and efforts by social media companies to prevent their platforms from being used as surveillance tools by blocking access to big data feeds.[438] Further, when automated tools were used, officers had to manually review the results just to decipher whether the applicant had been correctly matched to the social media account identified.[439]

In reviewing flagged items, FDNS officers are required to check for "national security indicators," but there seems to be a lack of clarity about what this means. In 2017, two years after the pilot programs were launched, DHS personnel reportedly expressed a need for a definition of what constitutes a "national security indicator in the context of social media."[440] The DHS inspector general noted a similar problem: his office was unable to evaluate specific policies and procedures for the pilot programs — because none existed.[441] Even more troubling, the inspector general found that DHS had simply failed to measure the effectiveness of the pilot programs, making them unsuitable as models for future initiatives.

According to the refugee program privacy impact assessment, five separate systems retain information for refugee processing, but none are described as containing social media data collected by DHS.[442] For example, the results of background checks, which may be informed by social media information, are stored in the State Department's refugee case management system, the Worldwide Refugee Admissions Processing System (WRAPS), but only in the form of a check's outcome ("clear" or "not clear").[443]

However, social media information is kept in a far-reaching system known as the Alien Files (A-Files), which covers every immigrant and some visitors to the United States.[444] USCIS is the main custodian of the system, with ICE and CBP regularly contributing to and using the data contained in it.[445] An individual's A-File is considered the official record of his or her immigration history and is used by a wide array of agency personnel for legal, fiscal, and administrative needs, such as naturalization and deportation proceedings.[446] A September 2017 notice in the Federal Register made clear that DHS collects and keeps social media information (handles, aliases, associated identifiable information, and search results) relating to immigrants, including legal permanent residents and naturalized citizens. In an email to the news site Gizmodo, DHS stated that "the notice does not authorize USCIS to search the social media accounts of naturalized citizens," which begs the question of whether other authorities are used to undertake such searches and leaves unaddressed the implications for people who have legal permanent resident status.[447] Regardless of whether new collection occurs, the 100-year A-File retention period means that DHS and other agencies can access and potentially use information gathered from social media long after an immigrant has completed the naturalization process. Despite questions from the press, DHS has not publicly clarified if and how this information could be used in the future.

To summarize, social media is used by USCIS in vetting people who apply for immigration benefits (such as students who become employed and change their visa status, or green card holders who become naturalized), and this information is retained in their A-Files. As discussed above, USCIS itself found that social media monitoring was not particularly helpful when it tested social media vetting for five programs. It has nonetheless proceeded with expanding its use of social media in several contexts, especially the vetting of refugee applicants and asylum seekers. It appears that such uses are focused on checking information provided by applicants, which may be justified for situations in which people seeking such status do not have documentation. But the ambiguous nature of social media raises concerns, as does the apparent targeting of certain — likely Muslim — applicants for such additional screening. Finally, as the inspector general's evaluation of these programs clearly indicates, DHS has made no effort to evaluate their effectiveness.

B. Vetting for the Controlled Application Review and Resolution Program

Social media reviews are also used in the Controlled Application Review and Resolution Program (CARRP), a secretive FDNS program instituted in 2008 for flagging and processing cases that present "national security concerns."[448] An individual who is placed on the CARRP track is essen-

tially blacklisted.[449] According to a study by the American Civil Liberties Union (ACLU), CARRP uses vague, overly broad, and discriminatory criteria and disproportionately targets Muslims and individuals from Muslim-majority countries.[450] The program has been challenged in court as "extra-statutory, unlawful, and unconstitutional."[451] A USCIS briefing book indicates that in July 2016, officers began screening social media accounts for Syrian and Iraqi CARRP cases specifically, though other documents suggest that social media is used to vet other populations as well.[452]

Applicants can be referred to CARRP in a variety of ways. Individuals who are flagged as known or suspected terrorists (including anyone in the FBI's overbroad Terrorist Screening Database, discussed above[453]) are automatically flagged as a national security concern and put on the CARRP track.[454] People can also be referred to CARRP at any stage of the screening and adjudicative process (e.g., when applying for citizenship or a green card) if they might present a "national security concern."[455] According to CARRP officer guidance, officers may utilize open-source research, including searching social media information, to identify an indicator of a national security concern.[456] The training handbook lists three broad categories of "non-statutory indicators" officers can consider to be indicative of a national security concern: "employment, training, or government affiliations" (e.g., foreign language expertise); "other suspicious activities" (e.g., unusual travel patterns); and "family members or close associates" (e.g., a roommate, coworker, or affiliate) who have been identified as national security concerns.[457]

While these factors could be relevant to national security, they also give USCIS officers great discretion and present serious due process and free speech concerns, particularly in the case of individuals who are in the United States and seeking adjustment of status.

C. Immigration Benefits Determinations

FDNS officers consult social media websites and commercial data sources, including Thomson Reuters's CLEAR database (discussed in the ICE section, above), during the screening of immigration benefit request forms, applications, or petitions.[458] According to information provided by FDNS to the DHS Privacy Office, data collected from social media during the benefit determination process is stored in the applicant's A-File, whether or not it was found to be derogatory, but applicants are given the opportunity to explain or refute any "adverse information" found through social media.[459] However, USCIS has not complied with the Privacy Office's 2012 recommendation to update the privacy impact assessments for several programs, including Deferred Action for Childhood Arrivals (DACA), to reflect that social media is used as a source of information and to address the privacy risks posed by such collection and how they would be mitigated.[460]

When someone applies for an immigration benefit (such as naturalization), the applicant's information is screened against data contained in USCIS, ICE, and other law enforcement databases for eligibility, fraud, and national security concerns.[461] In line with other DHS programs, USCIS is increasingly looking to automate many of the checks that it had previously performed manually. Since June 2017, USCIS and CBP have been working to gradually implement an interagency effort called "continuous immigration vetting."[462] Through this program, applicants applying for green cards or naturalization will have the biographical and biometric information they provide, as well as any information received by USCIS thereafter, automatically checked against CBP holdings. These checks will continue until the time of naturalization.[463] This new program is currently intended to uncover "potential national security concerns,"[464] although the recently published privacy impact assessment notes that the agency hopes to expand the process to vet for public safety concerns and fraud as well.[465]

Continuous immigration vetting relies on a connection between an existing USCIS screening tool called ATLAS[466] and CBP's ATS, which ingests and analyzes social media and other data from a plethora of sources. When someone applies for a benefit or information about an individual (such as an address) is updated, ATLAS automatically scans for potential matches to derogatory information in other government databases.[467] ATLAS itself analyzes information to detect patterns and trends; for example, it visually displays relationships among individuals on the theory that they could reveal potential ties to criminal or terrorist activity.[468]

With continuous immigration vetting, ATLAS also automatically sends any new information it receives over to ATS. ATS checks CBP holdings for matches to information about any individuals who have been flagged as a potential national security threat.[469] But ATS also stores the applicant or benefit holder's information for future use. Whenever derogatory information associated with an individual is added to a government database, ATS automatically checks for a "match and/or association" to the USCIS information and sends results back to ATLAS.[470] It is not clear that this new system will rely on social media. The privacy impact assessment notes that although ATS connects with multiple data sets, USCIS and CBP have tailored the initiative so that only "relevant" data sets are checked, although these are not identified.[471]

2. Administrative Investigations

FDNS conducts administrative investigations in order to procure additional information that can help determine an individual's eligibility for an immigration benefit. Administrative investigations seek to verify relationships that are the basis for an individual to receive an immigration

benefit, identify violations of the Immigration and Nationality Act, and identify other grounds of admissibility or removability.[472]

An officer can decide that an investigation is warranted on the basis of the results of a "manual review," which can be triggered by three mechanisms: a notification generated by ATLAS (when there is a match to one of its predefined rules), a fraud tip referral from the public or government officials, or a manual referral submitted by USCIS adjudications staff.[473] In order to officially open an administrative investigation after a manual review, the officer must determine that the tip is "actionable."[474] There are no publicly available criteria for this determination. The relevant privacy impact assessment notes only that investigations are performed due to suspected or confirmed fraud, criminal activity, or public safety or national security concern, or simply when a case is randomly selected for assessments to determine whether benefits have been obtained by fraud.[475] The broadness of these criteria suggests that the bar for opening an investigation is low and largely left to the officer's discretion.

As is the case with the screening of immigration benefits, FDNS may collect information from public sources, including social media, to serve as an additional check for other information collected during these investigations, support or refute any indication of fraudulent behavior, and identify threats to public safety or national security.[476] By way of example, FDNS is known to check an applicant's social media to help uncover "sham marriages."[477] That said, FDNS materials specify that an officer may not deny an immigration benefit, investigate benefit fraud, or identify public safety and national security concerns based solely on public source information.[478] Rather, such information may only be used to identify possible inconsistencies and must be corroborated with authoritative information on file with USCIS prior to taking action.[479] Any information found on a social media site and used during an investigation will be stored in both the applicant's hard-copy file and in the Fraud Detection and National Security Data System (FDNS-DS), regardless of whether it was found to be derogatory. If the information collected is found to be derogatory, the individual must be given the chance to explain or refute it, as is the FDNS standard with all derogatory information found from publicly available sources.[480]

As the above discussion shows, USCIS/FDNS has taken significant steps to incorporate social media into its various vetting and screening activities, including making admissibility and eligibility determinations for certain refugees and asylum seekers and for those placed on the CARRP track. There are questions about whether this vetting disproportionately targets Muslims and those from Muslim-majority countries. In refugee and asylum cases, social media could serve as a source of information for people who don't have many documents, but it could also serve as a way to weed out people due to ideological, racial, or religious prejudices or on the basis of misinterpretations. Administrative investigations too can use social media, although its use in that context is restricted to verification, and those affected have the opportunity to refute derogatory information. In line with other programs, USCIS is relying more and more on automation to support certain checks and screening processes.

Conclusion

Social media provides a huge trove of information about individuals — their likes and dislikes, their political and religious views, the identity of their friends and family, their health and mental state — that has proved irresistible for security and law enforcement agencies to collect and mine in the name of national security and public safety. Increasingly, DHS is vacuuming up social media information from a variety of sources, ranging from travelers' electronic devices to commercial databases, and using it to make decisions about who gets to come to the United States and the level of screening to which travelers are subjected. But there are serious questions about these programs: the evidence shows they are not effective in identifying risk, and they open the door to discrimination and the suppression of speech, association, and religious belief. Congress must fulfill its oversight responsibilities and require DHS both to come clean about the full extent of its social media surveillance and ensure that these programs are based on empirical evidence of effectiveness, safeguard against discrimination, and include robust privacy protections.

Appendix

DHS databases generally have a records retention schedule approved by the National Archives and Records Administration. The following appendix contains details on the retention schedules for the DHS systems that likely store social media data and other sensitive information.

DHS Component	Database/System	Retention Schedule
CBP	Automated Targeting System (ATS)	Risk assessments and other records in ATS are retained for 15 years, unless the information is "linked to active law enforcement lookout records . . . or other defined sets of circumstances," in which case the information is retained for "the life of the law enforcement matter."[481] This period may exceed the data retention requirements of the system from which the data originated, and therefore ATS may pass information to partners even after it has been deleted from other CBP databases.[482]
	Electronic System for Travel Authorization (ESTA)	CBP stores information from social media platforms collected during ESTA vetting in ATS.[483] ESTA application and vetting information is retained for a total of three years in active status (one year after the traveler's two-year travel authorization period expires), at which point the account information is archived for 12 years.[484] Data linked to active law enforcement lookout records continues to be accessible for the duration of the law enforcement activities to which it is related.[485]
	Analytical Framework for Intelligence (AFI)	Finished intelligence products in AFI are retained for 20 years.[486] Unfinished products that don't contain personal information are retained in AFI for 30 years; those that do must be recertified annually for continued relevance and accuracy.[487]
	CBP Intelligence Records System (CIRS)	Finished intelligence files are retained in CIRS for 20 years and raw, unevaluated information for 30 years.[488]
	Stand-alone IT systems (e.g., ADACS4)	Information collected during CBP's searches of electronic devices obtained pursuant to warrant, consent, or abandonment is stored in "stand-alone" technology systems (unconnected to other DHS databases). Information associated with arrests, detentions, and removals may be stored for up to 75 years, and information that does not lead to the arrest, detention, or removal of an individual may be stored for 20 years "after the matter is closed."[489]
TSA	Secure Flight	The passenger data from Secure Flight shared with CBP is deleted within seven days after the flight itinerary for passengers who do not require additional scrutiny. Passenger information on "potential" hits is retained in ATS for 15 years, 8 years after that information is removed from the Secure Flight system.[490] Confirmed matches to a watch list record or other derogatory information are retained for 99 years.[491] Data pertaining to individuals who match TSA's "rules" for lists such as the Silent Partner and Quiet Skies Lists are retained by both ATS and Secure Flight for seven years.[492] Secure Flight information that is linked to a border security, national security, significant health risk, or counterterrorism matter will be retained in ATS for the life of the matter.[493]

TSA Contd.	TSA Watch Lists	TSA Watch List master files are maintained for 30 years after the date of entry.[494]
	PreCheck	TSA retains information on individuals whose PreCheck applications were rejected because of their criminal history and places such individuals on a permanently retained list of passengers who are ineligible for PreCheck.[495] Information pertaining to an individual who is a match to a watch list will be retained for 99 years, or seven years after TSA learns that the individual is deceased, whichever is earlier.[496] Information pertaining to a PreCheck applicant who originally appeared to be a match to a watch list, but who was subsequently determined not to be a match, will be retained for seven years.[497] Information pertaining to an individual approved for PreCheck who no longer participates in the program is retained for one year after the request to stop participation in PreCheck is received.[498]
ICE	LeadTrac	Data stored in LeadTrac is retained for 75 years after the cases to which those records relate are closed.[499]
	Investigative Case Management (ICM) System	Under the proposed schedule, ICM records would be retained for 20 years from the end of the fiscal year in which a case is closed.[500] After 20 years, the information would either be destroyed or retained further under a new retention schedule if deemed necessary. However, cases would be permanently retained if deemed to be of significant "historical interest" (not defined). All ICM records will be treated as permanent records until a records retention schedule is approved.[501]
	FALCON-Search and Analysis (FALCON-SA)	Routinely ingested data is retained in accordance with the approved record retention schedule and SORN of those source systems. FALCON-SA data uploaded in an ad hoc manner, user-created visualizations, and search queries are retained in the system for the same length of time as the associated ICE case file. If there is no associated ICE case number, the retention period is 20 years.[502] Information from ATS pertaining to border crossings that is uploaded into FALCON-SA on an ad hoc basis is retained in FALCON-SA for 15 years after the relevant border crossing.[503]
	ICE Intelligence Records System (IIRS)	ICE is in the process of drafting a proposed record retention schedule for the sources maintained in the ICE Intelligence Records System.[504]
USCIS	Alien Files (A-Files)	An individual's A-File is retained for 100 years after his or her date of birth.[505]
	Fraud Detection and National Security Data System (FDNS-DS)	An individual's record is stored in FDNS-DS for 15 years after the date of his or her last interaction with FDNS personnel. However, records "related" (undefined) to the individual's A-File are transferred there and retained in accordance with the A-File retention schedule.[506]
DHS-Wide	DHS Data Framework	Data is retained in accordance with the retention schedules of source systems.[507]

Endnotes

1 U.S. Department of State, "60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa," 83 Fed. Reg. 13807, 13808 (March 30, 2018), https://www.regulations.gov/document?D=DOS-2018-0002-0001; Department of State, "60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration," 83 Fed. Reg. 13806, 13807 (March 30, 2018), https://www.regulations.gov/document?D=-DOS-2018-0003-0001; this proposed collection was approved on April 11, 2019. OMB, Notice of Office of Management and Budget Action, "Online Application for Nonimmigrant Visa," April 11, 2019, https://www.reginfo.gov/public/do/DownloadNOA?requestID=292517; OMB, Notice of Office of Management and Budget Action, "Electronic Application for Immigrant Visa and Alien Registration," April 11, 2019, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201808-1405-004. *See* also Brennan Center for Justice et al., Comments to Department of State, "Re: DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260, Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185," May 29, 2018, https://www.scribd.com/document/380580064/Brennan-Center-Urges-State-Department-to-Abandon-the-Collection-of-Social-Media-and-Other-Data-from-Visa-Applicants. Department of State visa applications are vetted using DHS's Automated Targeting System (ATS). DHS, Privacy Impact Assessment Update for the Automated Targeting System, DHS/CBP/PIA-006(e), January 13, 2017 (hereinafter ATS 2017 PIA), 8-9, 35, 59-60, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-december2018.pdf. The social media identifiers that the State Department collects via visa applications will be stored in the department's Consolidated Consular Database, which is ingested into ATS and becomes available to DHS personnel. ATS 2017 PIA, 3, 8-9, 12. For more on DHS involvement in State Department visa vetting, *see infra* text accompanying notes 118-131.

2 Section 208 of the E-Government Act of 2002 requires privacy impact assessments (PIAs) for all information technology that uses, maintains, or disseminates personally identifiable information or when initiating a new collection of personally identifiable information from 10 or more individuals in the public. E-Government Act of 2002, PL 107–347, December 17, 2002, 116 Stat 2899, https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf; DHS, "Privacy Compliance," accessed April 25, 2019, https://www.dhs.gov/compliance. DHS is required to publish or update existing privacy impact assessments when developing or procuring any new program or system that will handle or collect personally identifiable information; for budget submissions to the Office of Management and Budget that affect personally identifiable information; with pilot tests that affect personally identifiable information; when developing program or system revisions that affect personally identifiable information; or when issuing a new or updated rulemaking that involves the collection, use, and maintenance of personally identifiable information. Because revisions that affect personally identifiable information are common, DHS often issues multiple, updated privacy impact assessments for a single program or system.

3 A System of Records Notice (SORN) is required whenever the department has a "system of records" — a group of records from which information is retrieved by a personal identifier, such as one's name. SORNs, formal notices to the public published in the Federal Register, identify the purpose for which personally identifiable information is collected, what type of information is collected and from whom, how personally identifiable information is shared externally (routine uses), and how to access and correct any personally identifiable information maintained by DHS. DHS, "Privacy Compliance."

4 Pew Research Center, *Muslim Americans: No Signs of Growth in Alienation or Support for Extremism*, August 30, 2011, 108, http://www.pewresearch.org/wp-content/uploads/sites/4/legacy-pdf/Muslim-American-Report-10-02-12-fix.pdf (41 percent of American Muslims surveyed said they had not taken a flight in the past year, and 21 percent of those surveyed had been singled out by airport security, meaning that almost 36 percent of those surveyed who had taken a flight were singled out at security); Pew Research Center, *U.S. Muslims Concerned About Their Place in Society, but Continue to Believe in the American Dream*, July 26, 2017, 13, https://www.pewforum.org/wp-content/uploads/sites/7/2017/07/U.S.-MUSLIMS-FULL-REPORT-with-population-update-v2.pdf (reporting that 18 percent of American Muslims were singled out at airport security in the previous year, but not indicating the percentage of American Muslims who did not travel by air in the previous year); Faiza Patel, *Rethinking Radicalization*, Brennan Center for Justice, March 2011, https://www.brennancenter.org/sites/default/files/legacy/RethinkingRadicalization.pdf; Marc Sageman, *Misunderstanding Terrorism* (Philadelphia: University of Pennsylvania Press, 2016); Jamie Bartless, Jonathan Birdwell, and Michael King, *The Edge of Violence*, Demos, December 2010, https://www.demos.co.uk/files/Edge_of_Violence_-_full_-_web.pdf?1291806916.

5 *Cherri v. Mueller,* 951 F. Supp. 2d 918 (E.D. Mich. 2013).

6 Kari Huus, "Muslim Travelers Say They're Still Saddled With 9/11 Baggage," NBC News, September 9, 2011, http://www.nbcnews.com/id/44334738/ns/us_news-9_11_ten_years_later/t/muslim-travelers-say-theyre-still-saddled-baggage/#.XH61NcBKhpg.

7 ACLU and Muslim Advocates to DHS Inspector General Richard L. Skinner, December 16, 2010, https://www.aclu.org/letter/aclu-and-muslim-advocates-letter-department-homeland-security-inspector-general-richard.

8 *See* Amanda Holpuch and Ashifa Kassam, "Canadian Muslim Grilled About Her Faith and View on Trump at U.S. Border Stop," *Guardian*, February 10, 2017, https://www.theguardian.com/us-news/2017/feb/10/canadian-muslim-us-border-questioning; Emma Graham-Harrison, "US Border Agents Ask Muhammad Ali's Son, 'Are You a Muslim?' " *Guardian*, February 25, 2017, https://www.theguardian.com/us-news/2017/feb/25/muhammad-ali-son-detained-questioned-us-border-control; ACLU and Muslim Advocates to Skinner (highlighting the experiences of four other Muslim Americans who faced persistent religious questioning by CBP). *See* also Pew Research Center, *Muslim Americans*, 2.

9 *See* Faiza Patel and Harsha Panduranga, "Trump's Latest Half-Baked Muslim Ban," *Daily Beast*, June 12, 2017, https://www.thedailybeast.com/trumps-latest-half-baked-muslim-ban (noting that the administration's "extreme vetting" rules are aimed at the same pool of people as the Muslim ban); Harsha Panduranga, Faiza Patel, and Michael W. Price, *Extreme Vetting and the Muslim Ban*, Brennan Center for Justice, 2017, 2, 16, https://www.brennancenter.org/sites/default/files/publications/extreme_vetting_full_10.2_0.pdf. Brennan Center for Justice et al., Comments to Department of State, "Re: DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260, Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185," 7-8 (noting that the State Department's proposed collection of social media information from visa applicants would disproportionately burden Muslims). *See infra* note 120 and text accompanying notes 118-131.

10 DHS, "Demographic Profile of Perpetrators of Terrorist Attacks in the United States Since September 2001 Attacks Reveals Screening and Vetting Implications," 2018, https://assets.documentcloud.org/documents/4366754/Text-of-CPB-Report.pdf. The draft report, published by *Foreign Policy*, was produced at the request of the commissioner of U.S. Customs and Border Protection (CBP) to "inform United States foreign visitor screening, immigrant vetting and on-going evaluations of United States-based individuals who might have a higher risk of becoming radicalized and conducting a violent attack." It examined 29 individuals who, according to CBP, carried out terrorist incidents in the United States "driven by radical Sunni

Islamist militancy." Given the data set the report focused on, it unsurprisingly found that this cohort of people were mostly young, Muslim, and male. Ignoring the fact that hundreds of thousands of people who meet this description travel to the United States each year, CBP concluded that these characteristics provided a "baseline to identify at-risk persons." In fact, CBP even suggested that in addition to initial screenings, this enormous group of people should be "continuously evaluate[d]," for example when they applied for visa renewals or immigration benefits. Ibid., 4.

11 The Department of State issued more than 900,000 immigrant and nonimmigrant visas to individuals from Muslim-majority countries in FY 2018, which likely included hundreds of thousands of young Muslim men. *See* Department of State, Report of the Visa Office 2018, Table III and Table XVIII, https://travel.state.gov/content/travel/en/legal/visa-law0/visa-statistics/annual-reports/report-of-the-visa-office-2018.html.

12 *See infra* text accompanying note 428.

13 Elizabeth Stoycheff et al., "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects," *New Media & Society* 21, no. 3 (2018): 1-18, https://journals.sagepub.com/doi/abs/10.1177/1461444818801317. *See* also Dawinder S. Sidhu, "The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans," *University of Maryland Law Journal of Race, Religion, Gender and Class* 7, no. 2 (2007), https://core.ac.uk/download/pdf/56358880.pdf.

14 Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly* 93, no. 2 (2016): 296–311, https://journals.sagepub.com/doi/pdf/10.1177/1077699016630255. Similarly, in a survey of a representative sample of U.S. internet users, 62 percent reported that they would be much less or somewhat less likely to touch on certain topics if the government was watching, with 78 percent of respondents agreeing that they would be more cautious about what they said online. J. W. Penney, "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study," *Internet Policy Review* 6, no. 2 (2017), https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case. Another study measured how internet users in 11 countries reacted when they found out that DHS was keeping track of searches of terms that it regarded as suspicious, such as "state of emergency" and "drug war." Users were less likely to search using terms that they believed might get them in trouble with the U.S. government. Alex Marthews and Catherine Tucker, "Government Surveillance and Internet Search Behavior," February 17, 2017, https://ssrn.com/abstract=2412564. The study analyzed the search prevalence of select keywords compiled by the Media Monitoring Capability section of the National Operations Center of DHS. The list of keywords was publicized in 2012 as "suspicious" selectors that might lead to a particular user being flagged for analysis by the National Security Agency (NSA). *See* DHS, National Operations Center Media Monitoring Capability, "Analyst's Desktop Binder," 20, https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf. The authors later expanded their study to 41 countries and found that, for terms that users believed might get them in trouble with the U.S. government, the search prevalence fell by about 4 percent across the countries studied. Alex Marthews and Catherine Tucker, "The Impact of Online Surveillance on Behavior" in *The Cambridge Handbook of Surveillance Law,* ed. David Gray and Stephen E. Henderson (Cambridge: Cambridge University Press, 2017), 446. *See* also Human Rights Watch, *With Liberty to Monitor All: How Large-Scale U.S. Surveillance Is Harming Journalism, Law, and American Democracy*, July 28, 2014, https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and; PEN America Center, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, November 12, 2013, https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf (finding that 28 percent of writers reported "curtailed social media activities" in response to the Snowden revelations, 24 percent reported that they "deliberately avoided certain topics in phone or email conversations," and 16 percent reported that they "avoided writing or speaking about a particular topic").

15 *United States v. Jones,* 565 U.S. 400 (2012) (Sotomayor, J., concurring).

16 U.S. Citizenship and Immigration Services, "Social Media," in *U.S. Citizenship and Immigration Services Briefing Book,* (hereinafter USCIS Briefing Book) 181, https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf.

17 Office of Inspector General, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Redacted)*, February 27, 2017, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

18 Ibid. In a letter to the inspector general sent in response to the investigation, which was included in the publicly available report, DHS personnel noted that CBP also conducted a pilot program, with another soon to be initiated as of December 2016, but there is no publicly available information about either. Ibid., 7.

19 USCIS Briefing Book, 181.

20 Ibid., 183; DHS, Privacy Impact Assessment for the Fraud Detection and National Security Directorate, DHS/USCIS/PIA-013-01, December 16, 2014 (hereinafter FDNS 2014 PIA), 14, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-fdns-november2016_0.pdf.

21 USCIS Briefing Book, 183.

22 Ibid., 183.

23 Ibid., 183. Additional problems identified were the fact that refugee applicants had only a "minimal presence" on social media platforms accessible through social media monitoring programs and that the content was often not in English. Ibid., 181, 184.

24 Ibid., 184.

25 *See* Alexandra Olteanu et al., "Social Data: Biases, Methodological Pitfalls, and Ethical Boundaries," December 20, 2016, http://kiciman.org/wp-content/uploads/2017/08/SSRN-id2886526.pdf; Brennan Center for Justice et al., Comments to Department of State Regarding "Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants," May 18, 2017, https://www.brennancenter.org/sites/default/files/analysis/State%20Dept%20Information%20Collection%20Comments%20-%2051817_3.pdf.

26 *See* J. David Goodman, "Travelers Say They Were Denied Entry to U.S. for Twitter Jokes," *New York Times*, January 30, 2012, https://thelede.blogs.nytimes.com/2012/01/30/travelers-say-they-were-denied-entry-to-u-s-for-twitter-jokes/. FBI agents and even courts have erroneously interpreted tweets of rap lyrics as threatening messages. *See*, for example, Natasha Lennard, "The Way Dzhokhar Tsarnaev's Tweets Are Being Used in the Boston Bombing Trial Is Very Dangerous," *Fusion*, March 12, 2015, http://fusion.net/story/102297/the-use-of-dzhokhar-tsarnaevs-tweets-inthe-bostonbombing-trial-is-very-dangerous/; a Pennsylvania man was even sentenced to more than three years in prison for rap-style lyrics he posted to Facebook. The Supreme Court reversed the conviction in 2015. *United States v. Elonis*, 2011 WL 5024284 (E.D. Pa. Oct. 20, 2011), aff'd, 730 F.3d 321 (3d Cir. 2013), rev'd and remanded, 135 S. Ct. 2001 (2015), and aff'd, 841 F.3d 589 (3d Cir. 2016).

27 The total number of world languages is disputed. One widely cited estimate is that there are about 7,111 living languages, of which 3,995 have a developed writing system. These numbers are based on the definition of *language* (as opposed to *dialect*) as a speech variety that is not mutually intelligible with other speech varieties. *See* David M. Eberhard, Gary F. Simons, and Charles D. Fennig (eds.), *Ethnologue: Languages of the World*, 22nd ed. (Dallas, Texas: SIL International, 2019), https://www.ethnologue.com/enterprise-faq/how-many-languages-world-are-unwritten-0. The Department of State issues nonimmigrant visas to individuals from every country in the world annually. *See* Department of State, Report of the Visa Office

2018, Table XVIII: "Nonimmigrant Visas Issued by Nationality (Including Border Crossing Cards) Fiscal Year 2009–2018," https://travel.state.gov/content/dam/visas/Statistics/AnnualReports/FY2018AnnualReport/FY18AnnualReport%20-%20TableXVIII.pdf.

28 Brennan Center for Justice et al., Comments to Department of State Regarding "Notice of Information Collection Under OMB Emergency Review," 4-5.

29 Ben Conarck, "Sheriff's Office's Social Media Tool Regularly Yielded False Alarms," *Jacksonville,* May 30, 2017, https://www.jacksonville.com/news/public-safety/metro/2017-05-30/sheriff-s-office-s-social-media-tool-regularly-yielded-false.

30 Natasha Duarte, Emma Llanso, and Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis*, Center for Democracy and Technology, 2017, 5, https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf; Shervin Malmasi and Marcos Zampieri, "Challenges in Discriminating Profanity From Hate Speech," *Journal of Experimental & Theoretical Artificial Intelligence* 30, no. 2 (2018): 1-16, https://arxiv.org/pdf/1803.05495.pdf (reporting an 80 percent accuracy rate in distinguishing general profanity from hate speech in social media). Irene Kwok and Yuzhou Wang, "Locate the Hate: Detecting Tweets Against Blacks," *Proceedings of the 27th AAAI Conference on Artificial Intelligence* (2013), https://pdfs.semanticscholar.org/db55/11e90b2f4d650067ebf934294617eff81eca.pdf (finding an average 76 percent accuracy rate classifying hate speech on Twitter); Bo Han, "Improving the Utility of Social Media With Natural Language Processing" (PhD dissertation, University of Melbourne, February 2014), https://pdfs.semanticscholar.org/fd66/afb9d50c4770a529e7d125809053586b28dd.pdf (showing that natural language processing tools used to normalize "out-of-vocabulary" words, such as slang and abbreviations common on social media, into standard English achieved a 71.2 percent accuracy rate). In fact, accuracy itself is a somewhat slippery concept in these studies — it measures whether the tool came to the same conclusion that a human would have, but it does not take into account the possibility of human error or subjectivity. Duarte, Llanso, and Loup, *Mixed Messages?* 5, 17-18.

31 *See* Aaron Cantú and George Joseph, "Trump's Border Security May Search Your Social Media by 'Tone,' " *The Nation*, August 23, 2017, https://www.thenation.com/article/trumps-border-security-may-search-your-social-media-by-tone/ (noting that a senior DHS official touted the department's capacity to search its data sets, including social media data, "by tone"). Ahmed Abbasi, Ammar Hassan, and Milan Dhar, "Benchmarking Twitter Sentiment Analysis Tools," *Proceedings of the Ninth Language Resources and Evaluation Conference* (2014), https://www.researchgate.net/profile/Ammar_Hassan6/publication/273000042_Benchmarking_Twitter_Sentiment_Analysis_Tools/links/54f484d70cf2ba6150634593.pdf (finding that the best-performing sentiment analysis tools attain overall accuracies between 65 percent and 71 percent on average, while many low-performing tools yield accuracies below 50 percent); Mark Cieliebak et al., "A Twitter Corpus and Benchmark Resources for German Sentiment Analysis," *Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media* (2017): 49, https://pdfs.semanticscholar.org/a050/90ea0393284e83e961f199ea6cd03d13354f.pdf (finding that state-of-the-art systems for sentiment analysis in German achieve only around 60 percent accuracy in most cases, even when a system is trained and tested on the same corpus).

32 Daniel Preotiuc-Pietro, Ye Liu, Daniel J. Hopkins, Lyle Ungar, "Beyond Binary Labels: Political Ideology Prediction of Twitter Users," *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics* (2017), https://www.aclweb.org/anthology/P17-1068.

33 Diana Maynard, Kalina Bontcheva, and Dominic Rout, "Challenges in Developing Opinion Mining Tools for Social Media," *Proceedings of @NLP can u tag #user_generated_content?!* (2012), http://www.lrec-conf.org/proceedings/lrec2012/workshops/21.LREC2012%20NLP4UGC%20Proceedings.pdf#page=20 (showing that the accuracy of language and sentiment identification decreases when tools are used to analyze tweets because tweets tend to have greater language variation, tend to be less grammatical than longer posts, contain unorthodox capitalizations, and make frequent use of emoticons, abbreviations, and hashtags); Joan Codina and Jordi Atserias, "What Is the Text of a Tweet?" *Proceedings of @NLP can u tag #user_generated_content?!* (2012), http://www.lrec-conf.org/proceedings/lrec2012/workshops/21.LREC2012%20NLP4UGC%20Proceedings.pdf (arguing that the use of nonstandard language, emoticons, spelling errors, letter casing, unusual punctuation, and more makes applying natural language processing tools to user-generated social media content an unresolved issue); Dirk Von Grunigen et al., "Potential Limitations of Cross-Domain Sentiment Classification," *Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media* (2017), http://www.aclweb.org/anthology/W17-1103 (finding that sentiment analysis tools trained for one domain performed poorly in other domains). *See* generally Will Knight, "AI's Language Problem," *MIT Technology Review*, August 9, 2016, https://www.technologyreview.com/s/602094/ais-language-problem/.

34 Su Lin Blodgett and Brendan O'Connor, "Racial Disparity in Natural Language Processing: A Case Study of Social Media African-American English," *Proceedings of the Fairness, Accountability, and Transparency in Machine Learning Conference* (2017): 2, https://arxiv.org/pdf/1707.00061.pdf.

35 DHS, "DHS Transition Issue Paper: Screening and Vetting," 1, in *Strategic Issue Paper Summaries: Presidential Transition 2016–2017,* https://www.dhs.gov/sites/default/files/publications/TSA%20Presidential%20Transition%20Records.pdf#page=205 ("DHS is working to expand its current uses of social media to enhance existing vetting processes . . . [and] established a Social Media Task Force in December 2015 to examine current and potential uses of social media and how DHS could best expand its use").

36 George Joseph, "Extreme Digital Vetting of Visitors to the U.S. Moves Forward Under a New Name," *ProPublica*, November 22, 2017, https://www.propublica.org/article/extreme-digital-vetting-of-visitors-to-the-u-s-moves-forward-under-a-new-name.

37 Through the Visa Waiver Program, citizens of 38 mainly western European countries can apply to travel to the United States for business or tourism without obtaining a visa. For the full list of eligible countries, *see* CBP, "Frequently Asked Questions About the Visa Waiver Program (VWP) and the Electronic System for Travel Authorization (ESTA)," February 23, 2017, https://www.cbp.gov/travel/international-visitors/frequently-asked-questions-about-visa-waiver-program-vwp-and-electronic-system-travel. The Office of Management and Budget (OMB) approved CBP's proposal to collect the social media identifiers of visitors from Visa Waiver Countries on December 19, 2016. *See* OMB, Notice of Office of Management and Budget Action, "Arrival and Departure Record," December 19, 2016, https://www.reginfo.gov/public/do/DownloadNOA?requestID=275860*; see* also DHS Privacy Office, Notice of Privacy Act System of Records, CBP-009 Electronic System for Travel Authorization System of Records, 81 Fed. Reg. 60713 (September 2, 2016) (hereinafter ESTA SORN), https://www.gpo.gov/fdsys/pkg/FR-2016-09-02/pdf/2016-21210.pdf. DHS Office of Immigration Statistics, Table 28, "Nonimmigrant Admissions (I-94 Only) by Selected Category of Admission and Region and Country of Citizenship: Fiscal Year 2017," in *2017 Yearbook of Immigration Statistics*, https://www.dhs.gov/immigration-statistics/yearbook/2017/table28 (noting that the total number of travelers admitted to the United States through the Visa Waiver Program in fiscal year 2017 was 23,637,046).

38 *See* also Department of State, "Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants," 82 Fed. Reg. 20,956 (May 4, 2017), https://www.federalregister.gov/d/2017-08975; Department of State, "60-Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants," 82 Fed. Reg. 36,180 (August 3, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-08-03/pdf/2017-16343.pdf.

39 Department of State, "60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration"; Department of State, "60-Day Notice of Proposed Information Col-

lection: Application for Nonimmigrant Visa." *See* also Brennan Center for Justice et al., Comments to Department of State, "Re: DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260, Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185."

40 OMB, Notice of Office of Management and Budget Action, "Online Application for Nonimmigrant Visa"; OMB, Notice of Office of Management and Budget Action, "Electronic Application for Immigrant Visa and Alien Registration."

41 Beyond the "physical border," CBP also claims the authority to conduct electronic device searches at the "functional equivalent of the border" (such as an international airport within the United States) or the "extended border" (as when agents stop a person or vehicle that has recently crossed the border and is in the same state as when the border was crossed, and there is reasonable suspicion of criminal activity). Yule Kim, *Protecting the U.S. Perimeter: Border Searches Under the Fourth Amendment*, Congressional Research Service, June 29, 2009, 7-8, https://fas.org/sgp/crs/homesec/RL31826.pdf.

42 CBP, "CBP Releases Statistics on Electronic Device Searches," press release, April 11, 2017, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0. The fiscal year begins on October 1 of the prior year. So, for example, fiscal year 2017 ran from October 1, 2016, to September 30, 2017.

43 CBP, "CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics," press release, January 5, 2018, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

44 Geneva Sands, "Searches of Travelers' Electronic Devices Up Nearly 60 Percent," ABC News, January 5, 2018, https://abcnews.go.com/US/searches-travelers-electronic-devices-60-percent/story?id=52171977.

45 *See infra* text accompanying notes 243-256, 321-331, 415-417, 458.

46 *See supra* text accompanying notes 19-24.

47 *See infra* text accompanying notes 369-382. *See* also ICE, Directive No. 7-6.1, "Border Searches of Electronic Devices," August 18, 2009 (hereinafter ICE 2009 Directive, Border Searches of Electronic Devices), 2, https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

48 *See infra* text accompanying notes 102-104. *See* also DHS, Privacy Impact Assessment Update for the Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-007(g), September 1, 2016 (hereinafter ESTA 2016 PIA), 4, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-september2016.pdf.

49 ESTA 2016 PIA, 5.

50 *Data mining*, including social media data mining, is defined as conducting pattern-based queries, searches, or other analyses of one or more electronic databases to discover predictive patterns or anomalies. Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3(b)(1). *See* also DHS Privacy Office, *2017 Data Mining Report to Congress*, October 2018, 7, https://www.dhs.gov/sites/default/files/publications/2017-dataminingreport_0.pdf; DHS Management Directorate, Instruction Manual 262-12-001-01, "DHS Lexicon Terms and Definitions," October 16, 2017, 144-5, https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf (defining *data mining* as the "application of database technology and techniques to uncover hidden patterns, anomalies, and subtle relationships in data and to infer rules that allow for the prediction of future results").

51 Palantir developed CBP's Analytical Framework for Intelligence (AFI) and ICE's FALCON-Search and Analysis (FALCON-SA). For more on AFI's and FALCON-SA's analytical capabilities, *see infra* text accompanying notes 238-255 and 395-417, respectively. *See* also Spencer Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine," *Intercept*, March 2, 2017, https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/.

52 *See* DHS Privacy Office, Final Rule, CBP — 017 Analytical Framework for Intelligence (AFI) System of Records, 77 Fed. Reg. 47767, 47768 (August 10, 2012) (hereinafter AFI Final Rule), https://www.govinfo.gov/content/pkg/FR-2012-08-10/html/2012-19336.htm. The privacy impact assessment for ICE's FALCON-SA states that individuals seeking to correct any record contained in the system may submit a request, but it is unlikely that anyone would know that correction was needed, given that FALCON-SA is exempt from access requirements. Moreover, the privacy impact assessment clarifies that "all or some of the requested information may be exempt from correction pursuant to the Privacy Act." DHS, Privacy Impact Assessment Update for the FALCON Search & Analysis System, DHS/ICE/PIA-032(b) FALCON-SA, October 11, 2016 (hereinafter FALCON-SA 2016 PIA), 25-26, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-032-falcons-b-october2016.pdf.

53 *See*, for example, Erin Corbett, "Tech Companies Are Profiting Off ICE Deportations, Report Shows," *Fortune*, October 23, 2018, http://fortune.com/2018/10/23/tech-companies-surveillance-ice-immigrants/.

54 DHS defines *pattern analysis* as "identifying trends in activities or behaviors using prior actions and activities." DHS Management Directorate, "DHS Lexicon Terms and Definitions," 473. *See* also Joel B. Predd et al., *Using Pattern Analysis and Systematic Randomness to Allocate U.S. Border Security Resources,* RAND Corporation (2012), 1, https://apps.dtic.mil/dtic/tr/fulltext/u2/a558883.pdf (stating, in the context of border security, that "pattern and trend analysis refers to predictive methods that can identify regularities in the times, places, or tactics that interdicted border crossers have historically employed. For example, methods or tools of pattern and trend analysis may identify 'hot spots' — i.e., border zones or times of high or increased border activity — to ascertain where more resources could increase interdiction rates").

55 *See* ESTA 2016 PIA, 2; CBP, "Border Search of Electronic Devices," CBP Directive No. 3340-049A, January 4, 2018 (hereinafter CBP 2018 Directive), 5, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

56 USCIS, "USCIS Social Media & Vetting: Overview and Efforts to Date," March 2, 2017, 3, https://assets.documentcloud.org/documents/4341532/COW2017000400-FOIA-Response.pdf#page=56. This document is part of a series of internal reviews obtained by the *Daily Beast* via FOIA request that offer some information on these pilot programs and more broadly on USCIS's use of social media monitoring in its vetting efforts. *See* Aliya Sternstein, "Obama Team Did Some 'Extreme Vetting' of Muslims Before Trump, New Documents Show," *Daily Beast*, January 2, 2018, https://www.thedailybeast.com/obama-team-did-some-extreme-vetting-of-muslims-before-trump-new-documents-show.

57 ATS 2017 PIA, 4.

58 CBP, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the DHS Office of the General Counsel are supposed to conduct joint quarterly reviews of the risk-based rules used in ATS to ensure that the rules are appropriate, relevant, and effective and to assess whether privacy and civil liberties protections are adequate and consistently implemented. DHS Privacy Office, *2017 Data Mining Report to Congress*, 22. There is no publicly available information about these quarterly reviews, including whether they occur.

59 DHS Privacy Office, Final Rule, CBP — 006 Automated Targeting System of Records, 75 Fed. Reg. 5487 (February 3, 2010) (hereinafter ATS Final Rule), https://www.govinfo.gov/content/pkg/FR-2010-02-03/html/2010-2201.htm.

60 *See* Hayley Tsukayama and Jamie Williams, "If a Pre-Trial Risk Assessment Tool Does Not Satisfy These Criteria, It Needs to Stay Out of the Courtroom," Electronic Frontier Foundation, November 6, 2018, https://www.eff.org/deeplinks/2018/11/if-pre-trial-risk-assessment-tool-does-not-satisfy-these-criteria-it-needs-stay; Jesse Jannetta et al., *Examining Racial and Ethnic Disparities in Probation*

Revocation: Summary Findings and Implications From a Multisite Study, Urban Institute, April 2014, https://www.urban.org/sites/default/files/publication/22746/413174-Examining-Racial-and-Ethnic-Disparities-in-Probation-Revocation.PDF; Lori D. Moore and Irene Padavic, "Risk Assessment Tools and Racial/Ethnic Disparities in the Juvenile Justice System," *Sociology Compass* 5, no. 10 (2011): 850-858, https://coss.fsu.edu/subdomains/claudepeppercenter.fsu.edu_wp/wp-content/uploads/2015/04/Risk_Assessment_Juvies.pdf.

61 *See* Hearing on "Refugee Admissions FY 2018," Before the Subcommittee on Immigration and Border Security House Committee on the Judiciary, October 26, 2017 (written testimony of L. Francis Cissna, director, U.S. Citizenship and Immigration Services, DHS) (hereinafter Hearing on Refugee Admissions: Cissna Testimony), 5, https://www.uscis.gov/tools/resources/hearing-refugee-admissions-fy-2018-subcommittee-immigration-and-border-security-house-committee-judiciary-october-26-2017-uscis-director-l-francis-cissna; USCIS Briefing Book, 181.

62 Laura Koran and Tal Kopan, "US Increases Vetting and Resumes Processing of Refugees From 'High-Risk' Countries," CNN, January 29, 2018, https://www.cnn.com/2018/01/29/politics/us-refugee-vetting-measures/index.html.

63 For more on the monitoring of students who change their course of study to "sensitive" fields, *see infra* text accompanying notes 342-344.

64 For more on ICE's social media pilot programs, *see infra* text accompanying notes 342-359. Drew Harwell and Nick Miroff, "ICE Just Abandoned Its Dream of 'Extreme Vetting' Software That Could Predict Whether a Foreign Visitor Would Become a Terrorist," *Washington Post,* May 17, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/?utm_term=.57cbc2fc8442.

65 *See supra* text accompanying notes 10-11.

66 DHS Privacy Office, *2017 Data Mining Report to Congress*, 26.

67 "Statement of Work," ICE Contract #HSCEMD-14-C-00002 P00007, 31, https://www.brennancenter.org/sites/default/files/analysis/ICE%20FOIA%20Social%20Media%20Pilot%20Programs%20-%20BCJ.pdf.

68 *See supra* text accompanying notes 16-24.

69 *See*, for example, Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (London: SAGE Publications, 2014), 178; Victoria Sheriff, "Evaluating Preexisting Qualitative Research Data for Secondary Analysis," *Forum: Qualitative Social Research* 19, no. 2 (May 2018), http://www.qualitative-research.net/index.php/fqs/article/view/2821/4212.

70 CBP officers may use this information to vet the applicant and may also use it when travelers do not provide such information. *See* ESTA 2016 PIA, 2.

71 ESTA 2016 PIA, 5; DHS, Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices, DHS/CBP/PIA-008(a), January 4, 2018 (hereinafter CBP Electronic Border Searches 2018 PIA), 10, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp008-bordersearcheselectronicdevices-january2018.pdf. Information in ATS obtained from border searches does not include information from searches pursuant to warrant, consent, or abandonment. *See infra* text accompanying notes 178-194.

72 ATS 2017 PIA, 22-27, 35-37, 46-47, 58-60. For more on ATS and its interconnections with various DHS programs, *see infra* text accompanying notes 198-256, 258-297, 317, 336, 402-410, 466-471.

73 *See supra* notes iii-v acccompanying sidebar "Case Studies: Using Social Media to Target First Amendment–Protected Activity." The document listing targets displayed both U.S. and Mexican flags, as well as a seal for the International Liaison Unit, which coordinates intelligence between the two countries. Tom Jones, Mari Payton, and Bill Feather, "Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates," NBC San Diego, March 6, 2019, https://www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html.

74 Ibid.

75 Ibid.

76 ATS 2017 PIA, 44.

77 Memorandum from director, ICE Office of Investigations, to assistant directors, all deputy assistant directors, and all special agents in charge, "Field Guidance on Handling Detained or Seized Electronic Media From Persons of National Security Interest at Ports of Entry," March 5, 2007, 2, http://www.aclu.org/files/pdfs/natsec/laptopsearch/dhs_20100816_DHS000691-DHS000692.pdf.

78 DHS Privacy Office, Notice of Privacy Act System of Records, ICE–015 LeadTrac System of Records, 81 Fed. Reg. 52700 (August 9, 2016) (hereinafter LeadTrac SORN), https://www.regulations.gov/document?D=DHS-2016-0053-0001.

79 The Alien File, or A-File, is the official file for all immigration records. DHS Privacy Office, Notice of Modified Privacy Act System of Records, Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (October 18, 2017) (hereinafter A-Files SORN), https://www.gpo.gov/fdsys/pkg/FR-2017-09-18/pdf/2017-19365.pdf.

80 *See infra* text accompanying notes 118-131. Justice Department documents from April 2019 describing the expansion of social media identifier collection state that "information obtained from applicants . . . is considered confidential" though it "may be made available to a court or provided to a foreign government." However, the document does not mention the extensive sharing arrangement with ATS. Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Electronic Application for Immigrant Visa and Alien Registration," OMB Number 1405-0185, DS-260, April 11, 2019, 18, https://www.reginfo.gov/public/do/DownloadDocument?objectID=85760502. Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Application for Nonimmigrant Visa," OMB Number 1405-0182, DS-160 and DS-156, April 11, 2019, 19-20, https://www.reginfo.gov/public/do/DownloadDocument?objectID=85743802; ATS 2017 PIA 8-9.

81 *See generally* Rachel Levinson-Waldman, *What the Government Does With Americans' Data*, Brennan Center for Justice, October 8, 2013, https://www.brennancenter.org/sites/default/files/publications/Data%20Retention%20-%20FINAL.pdf.

82 Select Committee to Study Government Operations With Respect to Intelligence Activities, Final Report, S. Rep. No. 94-755, pt. 3, 778 (1976), https://www.intelligence.senate.gov/sites/default/files/94755_III.pdf.

83 ATS 2017 PIA, 14.

84 ESTA 2016 PIA, 6 (noting that, after being retained for up to three years, ESTA application data must then enter archive status). However, it does not appear that ATS adheres to this rule. ATS 2017 PIA, 77.

85 DHS, Privacy Impact Assessment for the DHS Data Framework — Interim Process to Address an Emergent Threat, DHS/ALL/PIA-051, April 15, 2015 (hereinafter Data Framework — Interim Process PIA), 8, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-dataframework-april2015.pdf. *See infra* text accompanying notes 218-231.

86 The Data Framework operates under an interim process in which data is not tagged with the relevant retention restrictions. Ibid., 8-9. *See infra* text accompanying note 225.

87 A-Files SORN, 43564.

88 CBP screens travelers before they board a flight on a U.S.-registered airline anywhere in the world, regardless of whether or not the flight touches down in the United States or flies in U.S. airspace. DHS, Privacy Impact Assessment Update for the Automated Targeting System — TSA/CBP Common Operating Picture, Phase II, DHS/CBP/PIA-006(d), September 16, 2014 (hereinafter ATS-TSA PIA, Common Operating Picture, Phase II), 3, https://www.dhs.gov/sites/default/

files/publications/privacy_pia_cbp_tsacop_09162014.pdf. CBP and TSA cooperate closely in conducting screenings. *See infra* text accompanying notes 277-297 for more on CBP's preflight screening and watch listing.

89 ESTA, U.S. Travel Authorization Application, "Visa Waiver Countries," http://www.esta.us/visa_waiver_countries.html. However, if an individual traveled to Iran, Iraq, Sudan, Syria, Libya, Somalia, or Yemen on or after March 1, 2011, he or she is ineligible for the program. CBP, "Visa Waiver Program Improvement and Terrorist Travel Prevention Act, Frequently Asked Questions," https://www.cbp.gov/travel/international-visitors/visa-waiver-program/visa-waiver-program-improvement-and-terrorist-travel-prevention-act-faq.

90 *See* DHS Office of Immigration Statistics, Table 28, "Nonimmigrant Admissions (I-94 Only)."

91 Visa waiver applicants who do not submit the online ESTA form must complete an I-94W form when they arrive at the border, but they may be denied boarding, experience delayed processing, or be denied admission. CBP, "Frequently Asked Questions About the Visa Waiver Program (VWP) and the Electronic System for Travel Authorization (ESTA)," 2016.

92 ESTA 2016 PIA, 5. If an applicant does not qualify for the Visa Waiver Program, he or she must go through the nonimmigrant visa application process. CBP, "ESTA Application Denied," June 14, 2017, https://help.cbp.gov/app/answers/detail/a_id/1074/~/esta-application-denied.

93 DHS, "National Targeting Center: Passenger Operations," in *CBP Presidential Transition Records*, 5, https://www.dhs.gov/sites/default/files/publications/CBP%20Presidential%20Transition%20Records.pdf.

94 The attack by a VWP traveler killing one American resident occurred in 1990. Alex Nowrasteh, "Terrorists by Immigration Status and Nationality: A Risk Analysis, 1975-2017," Policy Analysis no. 866, May 7, 2019, https://www.cato.org/publications/policy-analysis/terrorists-immigration-status-nationality-risk-analysis-1975-2017.

95 ESTA 2016 PIA, 2. OMB, Notice of Office of Management and Budget Action, "Arrival and Departure Record" (noting that the social media identifier collection was approved on December 19, 2016). ESTA privacy documents note that providing social media information is "optional" for visa waiver applicants and omission will not affect their eligibility determination. ESTA SORN; DHS Privacy Office, Notice of Privacy Act System of Records, CBP — 009 Electronic System for Travel Authorization System of Records Notice, 81 Fed. Reg. 39680 (June 17, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-06-17/pdf/2016-14422.pdf. Regardless, applicants will likely feel pressure to comply. The ESTA form requires applicants to affirm that the information they have supplied is "true and correct." If they provide their username for one social media account but not for another, they may worry that their submission will be perceived as untruthful. *See* Brennan Center for Justice, Comments to CBP, August 22, 2016, https://www.brennancenter.org/sites/default/files/321910883-Brennan-Center-Submits-Comments-on-DHS-Plan-to-Collect-Social-Media-Information.pdf.

96 ESTA 2016 PIA, 2. CBP, Frequently Asked Questions, "How will CBP use my social media information collected through the additional question that was added to the ESTA application in December 2016?" https://esta.cbp.dhs.gov/esta/application.html?execution=e2s1.

97 ESTA 2016 PIA, 2.

98 *See supra* text accompanying notes 16-24.

99 The information is also used for "law enforcement vetting purposes," which could mean ensuring that there are no criminal charges against an ESTA applicant but could also be construed more broadly, and for "eligibility determinations," which presumably would reflect the legal parameters of immigration law. ESTA 2016 PIA, 2.

100 ESTA 2016 PIA, 4.

101 *See*, for example, Kavitha Surana, "How Racial Profiling Goes Unchecked in Immigration Enforcement," *ProPublica*, June 8, 2018, https://www.propublica.org/article/racial-profiling-ice-immigration-enforcement-pennsylvania. According to a former ICE agent, officers use observations about people's demeanor to evaluate whether they might be undocumented, such as "when people speak only Spanish" or "appear nervous when encountered by an immigration officer." Ibid.

102 ESTA 2016 PIA, 4.

103 Ibid., 5.

104 Ibid., 3-4.

105 DHS, Directive 110-01, "Privacy Policy for Operational Use of Social Media," June 8, 2012, 8, https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf.

106 CBP, Privacy Compliance Review of the U.S. Customs and Border Protection Electronic System for Travel Authorization, October 27, 2017, 8, https://www.dhs.gov/sites/default/files/publications/CBP-ESTA%20PCR%20final%20report%2020171027.pdf.

107 ESTA 2016 PIA, 4-5.

108 The detailed CBP rules implementing the directive, which were obtained by the Brennan Center via FOIA, confirm that its officers can undertake masked monitoring, but the triggers and rules for utilizing this technique are redacted. DHS, "DHS Operational Use of Social Media," July 24, 2012, 5, https://www.brennancenter.org/sites/default/files/analysis/FOIA-CBP%20Social%20Media%20Use%20Template.pdf.

109 ESTA 2016 PIA, 5.

110 ATS 2017 PIA, 25. The role of ATS in preflight and watch list screening is described in more detail in the TSA section; *see infra* text accompanying notes 258-297. Various records from ATS are shared with CBP's Analytical Framework for Intelligence (AFI), which is used to create various analytical products. *See* DHS, Privacy Impact Assessment Update for the Analytical Framework for Intelligence (AFI), DHS/CBP/PIA-010(a), September 1, 2016 (hereinafter AFI 2016 PIA), 1, 3, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-010-a-afi-2016.pdf; *see infra* text accompanying notes 236-255.

111 ESTA SORN, 60717.

112 *See* National Security Presidential Memorandum (NSPM-9), "Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise," February 6, 2018, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-optimizing-use-federal-government-information-support-national-vetting-enterprise/; DHS, "Plan to Implement the Presidential Memorandum on Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise," August 5, 2018, https://www.dhs.gov/sites/default/files/publications/NSPM-9%20Implementation%20Plan.pdf; DHS, Privacy Impact Assessment for the National Vetting Center (NVC), DHS/ALL/PIA-072, December 11, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall072-nvc-december2018.pdf.

113 DHS, "Plan to Implement the Presidential Memorandum," 13.

114 Information may be shared with any "appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order." ESTA SORN, 60717.

115 For more on the NCTC, *see* National Counterterrorism Center, *Today's NTC*, August 2017, 3, https://www.dni.gov/files/NCTC/documents/features_documents/NCTC-Primer_FINAL.pdf; Sari Horwitz and Ellen Nakashima, "New Counterterrorism Guidelines Permit Data on U.S. Citizens to Be Held Longer," *Washington Post*, March 22, 2012, https://www.washingtonpost.com/world/national-security/new-counterterrorism-guidelines-would-permit-data-on-us-citizens-to-be-held-longer/2012/03/21/gIQAFLm7TS_story.html?utm_term=.d97d67cd488f. DHS, Privacy Impact Assessment Update for the Electronic System for Travel Authorization, DHS/CBP/

PIA-007(c), June 5, 2013 (hereinafter ESTA 2013 PIA), 3-4, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-update-20130606_0.pdf. The memorandum of understanding was updated in 2013. Ibid., 5. *See* also Rachel Levinson-Waldman, *What the Government Does With Americans' Data*, 20 (noting that NCTC has access to data related to international travel and immigration benefits, as well as financial data, none of which is related to terrorism).

116 ESTA 2013 PIA, 2-4, n8.

117 *See supra* text accompanying notes 109-110.

118 Visa application data from two Department of State sources, the Consular Consolidated Database and the Consular Electronic Application Center, are compared with existing information in CBP's ATS for vetting purposes. ATS 2017 PIA, 8-9, 59-60. The Consular Consolidated Database contains records of all visa applications, beginning from the mid-1990s — a total of more than 140 million records. Ruth Ellen Wasem, *Immigration: Visa Security Policies*, Congressional Research Service, R43589, 2015, 6, https://fas.org/sgp/crs/homesec/R43589.pdf. The Consular Consolidated Database receives information from ATS indicating whether or not DHS identified derogatory information about the visa applicant. If ATS identifies derogatory information relating to an application, that application is referred for manual review. If, following manual review, an applicant is determined to be eligible for a visa, an updated response is sent to the Consular Consolidated Database. ATS 2017 PIA, 34.

119 Department of State, "Notice of Information Collection Under OMB Emergency Review."

120 Ibid. The estimate in the Federal Register notice that about 65,000 people will be subject to "increased scrutiny" closely tracks the roughly 68,000 nonimmigrant visas issued in 2016 to nationals of the seven countries included in the first travel ban. *See* Department of State, Bureau of Consular Affairs, Table XVIII: "Nonimmigrant Visas Issued by Nationality (Including Border Crossing Cards), Fiscal Year, 2007–2016," https://travel.state.gov/content/dam/visas/Statistics/AnnualReports/FY2016AnnualReport/FY16AnnualReport-TableXVIII.pdf. Additionally, the State Department's first attempt at implementing the new rule requiring some categories of visa applicants to provide their social media identifiers — which was halted due to litigation — directed consular officials to implement these measures for all nationals of the initial Muslim ban countries. Department of State, "Implementing Immediate Heightened Screening and Vetting of Visa Applications," 17 STATE 24324, ¶ 9-14, http://live.reuters.com/Event/Live_US_Politics/791246151. *See* also Alex Nowrasteh, "New Trump Executive Order Fails Cost-Benefit Test," *Cato at Liberty* (blog), Cato Institute, September 25, 2017, https://www.cato.org/blog/new-trump-executive-order-fails-cost-benefit-test (noting that, had the third iteration of the Muslim ban — Presidential Proclamation 9645 — been in effect in 2016, "it would have halted the travel, migration and immigration of roughly 66,000 people"); Patel and Panduranga, "Trump's Latest Half-Baked Muslim Ban."

121 Department of State, "60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration"; Department of State, "60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa." The social media identifiers will be collected via the visa application forms DS-156, 160, and 260, all three of which are stored in the Consular Consolidated Database. Department of State, Bureau of Consular Affairs Visa Services, "Records Disposition Schedule," https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-state/rg-0084/n1-084-09-002_sf115.pdf. *See* also Brennan Center for Justice et al., Comments to Department of State, "Re: DS-160 and DS-156, Application for Nonimmigrant Visa, OMB Control No. 1405-0182; DS-260, Electronic Application for Immigrant Visa and Alien Registration, OMB Control No. 1405-185."

122 OMB, Notice of Office of Management and Budget Action, "Online Application for Nonimmigrant Visa"; OMB, Notice of Office of Management and Budget Action, "Electronic Application for Immigrant Visa and Alien Registration." *See* Department of State, Consolidated Nonimmigrant Visa Application, DS-0156, 2, https://www.regulations.gov/contentStreamer?documentId=-DOS-2018-0002-0001&attachmentNumber=2&contentType=pdf; Department of State, Online Immigrant Visa and Alien Registration Application, OMB Submission, DS-260, 13, https://www.reginfo.gov/public/do/DownloadDocument?objectID=85760401.

123 *See* Department of State, Consolidated Nonimmigrant Visa Application, DS-0156, 2; Department of State, Online Immigrant Visa and Alien Registration Application, DS-260, 13.

124 Department of State, Consolidated Nonimmigrant Visa Application, DS-0156, 2; Department of State, Online Immigrant Visa and Alien Registration Application, DS-260, 13; Department of State, "60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration"; Department of State, "60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa."

125 Under applicable U.S. law, an applicant may be ineligible for a visa on grounds, among others, related to health, crime, labor, terrorism, and prior immigration violations. *See* 8 U.S.C. § 1182(a); 8 U.S.C. § 1184(b); 8 U.S.C. § 1158(d)(6). Section 1202(a) provides that an applicant for an immigrant visa must "state his full and true name, and any other name which he has used or by which he has been known; age and sex; the date and place of his birth; and such additional information necessary to the identification of the applicant and the enforcement of the immigration and nationality laws as may be [required] by regulations prescribed." 8 U.S.C.A. § 1202(a). Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Electronic Application for Immigrant Visa and Alien Registration," 10-11; Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Application for Nonimmigrant Visa," 11.

126 Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Application for Nonimmigrant Visa," 20; Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Electronic Application for Immigrant Visa and Alien Registration," 18-19.

127 Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Application for Nonimmigrant Visa," 8-9, 20; Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Electronic Application for Immigrant Visa and Alien Registration," 8, 19.

128 ATS 2017 PIA, 3, 35-37. The Justice Department's supporting statement describing the expansion of social media identifier collection states that "information obtained from applicants . . . is considered confidential" though it "may be made available to a court or provided to a foreign government." *See* Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Electronic Application for Immigrant Visa and Alien Registration," 18. All Consular Consolidated Database (CCD) visa record reports are subject to confidentiality requirements and cannot be shared without the permission of the Department of State. Department of State, Privacy Impact Assessment (PIA), Consular Consolidated Database (CCD), Version 04.00.00, July 17, 2015 (hereinafter CCD 2015 PIA), 8, https://www.state.gov/documents/organization/242316.pdf. However, the supporting statement does not mention the extensive sharing arrangement with ATS, and it remains unclear how far social media identifiers and other CCD information may spread within DHS and to external agencies after being ingested into ATS. The CCD PIA from 2015, which predates the social media identifier collection, lists CBP as an external organization with which CCD may share information but does not address privacy concerns related to the extensive sharing of personally identifiable information with CBP. CCD 2015 PIA, 11. *See* also ATS 2017 PIA, 8, 11. In 2016, the CCD was found to have glaring security vulnerabilities. Mike Levine and Justin Fishel, "Exclusive: Security Gaps Found in Massive Visa Database," ABC News, March 31, 2016, https://abcnews.go.com/US/exclusive-security-gaps-found-massive-visa-database/story?id=38041051.

129 Department of State, "Supporting Statement for Paperwork Reduction Act Submission: Application for Nonimmigrant Visa," 2; De-

partment of State, "Supporting Statement for Paperwork Reduction Act Submission: Electronic Application for Immigrant Visa and Alien Registration," 2.

130 Department of State, Notice of a Modified System of Records, Visa Records, State-39, 83 Fed. Reg. 28062 (June 15, 2018) (hereinafter Visa SORN), https://www.govinfo.gov/content/pkg/FR-2018-06-15/pdf/2018-12871.pdf. Agencies such as the CIA and the Department of Defense may soon have access to State Department visa information through the National Vetting Center (NVC), and the State Department is likely to share the visa data it collects with DHS through the NVC as well. *See supra* text accompanying notes 111-114; "Plan to Implement the Presidential Memorandum," 8. *See* National Security Presidential Memorandum, "Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise."

131 *See infra* text accompanying notes 198-256.

132 CBP 2018 Directive, 1.

133 Ibid.

134 The relevant CBP directive is somewhat confusing in regard to information stored remotely. On one hand, it states that officers "may not intentionally use the device to access information that is solely stored remotely" for CBP basic or advanced searches. CBP 2018 Directive, 4; CBP Electronic Border Searches 2018 PIA, 8. But the same directive notes that "an advanced search is any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." CBP 2018 Directive, 5.

135 The website USASpending lists CBP contracts for UFEDs totaling $1,594,366. CBP contract with Cellebrite, May 12, 2009–September 25, 2018, USASpending, https://www.usaspending.gov/#/search/134309b58a47879206e3a328a4e47ec5. *See* Jose Pagliery, "Cellebrite Is the FBI's Go-To Phone Hacker," CNN, April 1, 2016, https://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/index.html; "The Feds Can Now (Probably) Unlock Every iPhone Model in Existence," *Forbes*, February 26, 2018, https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#70d4f042667a; Cellebrite, "UFED Cloud Analyzer," https://www.cellebrite.com/en/products/ufed-cloud-analyzer/.

136 CBP, "CBP Releases Statistics on Electronic Device Searches."

137 CBP, "CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics."

138 CBP 2018 Directive, 3.

139 While DHS itself does not provide a breakdown, ABC News reports that about 80 percent of searches are of noncitizens, which would mean that in fiscal year 2017, CBP conducted more than 6,000 searches of devices belonging to U.S. citizens. Sands, "Searches of Travelers' Electronic Devices Up Nearly 60 Percent."

140 Amended Complaint, *Alasaad v. Nielsen*, 2017 WL 4037436 (D.Mass. Sept. 13, 2017), https://www.eff.org/files/2017/09/13/7._amended_complaint.pdf.

141 Ibid.

142 CBP 2018 Directive, 4-5.

143 *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013).

144 DHS, Privacy Impact Assessment for CBP and ICE Border Searches of Electronic Devices, August 25, 2009 (hereinafter ICE/CBP Electronic Device Searches 2009 PIA), 4, https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_laptop.pdf; ICE 2009 Directive, Border Searches of Electronic Devices, 2.

145 CBP Electronic Border Searches 2018 PIA, 6.

146 CBP 2018 Directive, 4. This restriction was absent from CBP's original electronic border search directive (2009). In response to questions posed by Senator Ron Wyden, CBP clarified that its agents do not access information found on remote servers during electronic device searches, but it did not state how agents were to ensure this in practice (e.g., disabling connectivity via airplane mode). CBP, "Due Diligence Questions for Kevin McAleenan, Nominee for Commissioner of U.S. Customs and Border Protection (CBP)," June 20, 2017, 3, https://www.washingtonpost.com/blogs/the-switch/files/2017/07/cbp-wyden.pdf.

147 The officer may disconnect the device herself or conduct the search without the individual present if there are national security, law enforcement, officer safety, or other operational considerations. CBP 2018 Directive, 5, 6.

148 Esha Bhandari, staff attorney, American Civil Liberties Union, email message to authors, August 13, 2018.

149 CBP 2018 Directive, 6.

150 Ibid.

151 Unless unspecified "extenuating circumstances" exist, CBP policy states that devices should not be detained for longer than five days. CBP 2018 Directive, 7.

152 *See* Seth Schoen, Marcia Hofmann, and Rowan Reynolds, "Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices," Electronic Frontier Foundation, December 2011, 5, https://www.eff.org/files/eff-border-search_2.pdf. There are a variety of reasons why a noncitizen may be denied entry. *See* Immigration and Nationality Act § 212(a), 8 U.S.C. § 1182 (2010). *See* also Daniel Victor, "What Are Your Rights if Border Agents Want to Search Your Phone?" *New York Times*, February 14, 2017, https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html.

153 CBP 2018 Directive, 5. In 2007, CBP began using external equipment for advanced searches at four ports of entry. As of July 2017, such use had expanded to 67 ports of entry. Office of Inspector General, DHS, *CBP's Searches of Electronic Devices at Ports of Entry*, December 3, 2018 (hereinafter OIG 2018 Electronic Device Report), 9, https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf.

154 *See supra* text accompanying notes 134-135.

155 CBP 2018 Directive, 5.

156 Ibid.

157 CBP Electronic Border Searches 2018 PIA, 3, 6.

158 OIG 2018 Electronic Device Report, 4.

159 CBP 2018 Directive, 7.

160 Ibid.

161 Ibid., 9-10. CBP can retain such information so long as "the retention is consistent with the applicable system of records notice." Ibid.

162 Ibid., 10; A-Files SORN, 43564.

163 CBP Electronic Border Searches 2018 PIA, 10. DHS Privacy Office, *2017 Data Mining Report to Congress,* 16; ATS 2017 PIA, 1.

164 CBP Electronic Border Searches 2018 PIA, 15. CBP may also share the device or information from the device with third parties to receive technical assistance in accessing the device's contents. In general, such assisting agencies are permitted to retain the information only as long as necessary to provide such assistance, unless the devices are seized on the basis of probable cause or if an assisting federal agency elects to retain it under its own independent legal authority. CBP 2018 Directive, 11.

165 OIG 2018 Electronic Device Report, 1. CBP's original policy from 2009 was in effect at the time of this review. Ibid., 5.

166 Ibid., 1.

167 Ibid., 8.

168 Ibid., 9. The report describes CBP's forensic electronic device searches as a "pilot program," which was rolled out in 2009, but it is clear given the January 2018 privacy impact assessment update that forensic searches are now a permanent part of CBP's border searches.

169 CBP 2018 Directive, 12.

170 Complaint for Injunction Relief, *Electronic Privacy Information Center v. U.S. Customs and Border Protection*, No. 1:19-cv-00279 (D.D.C. Feb. 1, 2019), https://epic.org/foia/cbp/border-device-search-audits/Complaint.pdf.

171 *See*, for example, Holpuch and Kassam, "Canadian Muslim Grilled About Her Faith"; Sedria Renee, "Muhammad Ali Jr. on Airport Detainment: 'I'm Not American?' " NBC News, February 27, 2017, https://www.nbcnews.com/news/us-news/muhammad-ali-jr-airport-detainment-i-m-not-american-n726246. *See* also Complaint for Injunctive and Declaratory Relief and Damages, *El Ali et al. v. Sessions et al*., No. 8:18-cv-02415-PX (D. Md. Aug. 8, 2018), https://papersplease.org/wp/wp-content/uploads/2018/08/watchlist-complaint-8AUG2018.pdf; *American Civil Liberties Union et al. v. TSA*, No. 1:15-cv-02061-JPO (S.D.N.Y. 2015), https://www.aclu.org/legal-document/aclu-v-tsa-complaint; Michael S. Schmidt and Eric Lichtblau, "Racial Profiling Rife at Airport, U.S. Officers Say," *New York Times*, August 11, 2012, http://nyti.ms/lGsuvBV.

172 *See*, for example, Theodore Schleifer, "Donald Trump: 'I Think Islam Hates Us,' " CNN, March 10, 2016, https://www.cnn.com/2016/03/09/politics/donald-trump-islam-hates-us/index.html; Philip Bump and Aaron Blake, "Donald Trump's Dark Speech to the Republican National Convention, Annotated," *Washington Post*, July 21, 2016, https://www.washingtonpost.com/news/the-fix/wp/2016/07/21/full-text-donald-trumps-prepared-remarks-accepting-the-republican-nomination/?utm_term=.3d7121332501; *Meet the Press*, July 24, 2016, NBC News, https://www.nbcnews.com/meet-the-press/meet-press-july-24-2016-n615706.

173 Cyrus Farivar, "Woman: My iPhone Was Seized at Border, Then Imaged — Feds Must Now Delete Data," *Ars Technica*, August 23, 2018, https://arstechnica.com/tech-policy/2018/08/woman-my-iphone-was-seized-at-border-then-imaged-feds-now-must-delete-data/.

174 Brief of Petitioner, *Lazoja v. Nielsen*, No. 18-cv-13113 (D.N.J. Aug. 23, 2018), https://assets.documentcloud.org/documents/4781285/Document.pdf.

175 Ibid., 15.

176 Cyrus Farivar, "Feds Took Woman's Iphone at Border, She Sued, Now They Agree to Delete Data," *Ars Technica*, October 31, 2018, https://arstechnica.com/tech-policy/2018/10/feds-agree-to-delete-data-seized-off-womans-iphone-during-border-search/.

177 *See infra* text accompanying notes 195-256.

178 DHS, Privacy Impact Assessment for U.S. Border Patrol Digital Forensics Programs, April 6, 2018 (hereinafter CBP 2018 Digital Forensics PIA), 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp053-digitalforensics-april2018.pdf.

179 Ibid., 2.

180 Catherine E. Shoichet, "The U.S. Border Is Bigger Than You Think," CNN, May 24, 2018, https://www.cnn.com/2018/05/23/us/border-zone-immigration-checks/index.html. CBP officials claim authority to board and search "any railway car, aircraft, conveyance, or vehicle" anywhere within a reasonable distance from any external boundary of the United States." 8 U.S.C. § 1357(a)(3). Reasonable distance is defined as "100 air miles from any external boundary of the United States . . ." 8 C.F.R. § 287.1(a)(1).

181 CBP 2018 Digital Forensics PIA, 2.

182 CBP does not define *accurate* or *reliable.* Ibid., 10.

183 Ibid. There is an exception for cases where the evidence itself indicates a violation of law — for instance, child pornography — in which case action presumably could be taken solely on the basis of information retrieved from the device. Ibid.

184 Ibid., 8.

185 Ibid., 3.

186 In the case of searches authorized by a warrant, information must be within the scope of the warrant. Ibid., 4.

187 Ibid., 4. (Emphasis theirs.)

188 Ibid., 4-5. These tools include "timeframe analysis, which can help in determining when data were entered, modified, or deleted from a device"; "detection recovery of concealed data"; "correlation of files to installed applications, examination of drive file structure, and review of metadata"; and "reviews to help to identify individuals who created, modified, or accessed a file." Ibid., 4-5. If the analytical results produced by a system "develop leads, identify trends associated with illicit activity, and further law enforcement actions," they will be included in an enforcement case file or law enforcement intelligence product, such as a field intelligence report, "for dissemination." Ibid., 11.

189 Ibid., 4. While the privacy impact assessment does not specify that ADACS4 includes social media data, it seems likely given that such information is typically found on electronic devices.

190 Ibid., 7. In the special case of information obtained through a search warrant that is subsequently found to be outside the scope of that warrant, it will be deleted from the system once the case or trial is complete. Ibid., 5.

191 Ibid., 14.

192 Ibid., 14. If a recipient wants to re-disseminate information, it must obtain permission from CBP, though permission is sometimes granted when CBP information is first shared. Ibid., 14.

193 Carmen Sesin, "Two-Thirds of Americans Live in a Border Zone; What Are Their Rights?" NBC News, January 26, 2018, https://www.nbcnews.com/news/latino/two-thirds-americans-live-border-zone-what-are-their-rights-n841141.

194 *See supra* text accompanying notes 186-192.

195 ATS 2017 PIA, 2-3, 82-83.

196 DHS Management Directorate, "DHS Lexicon Terms and Definitions," 473.

197 *See* DHS, Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI), June 1, 2012 (hereinafter AFI 2012 PIA), 4, https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf.

198 While the rules underlying risk assessments are subject to quarterly reviews to assess whether privacy and civil liberties protections are adequate and consistently implemented, there is no publicly available information about these quarterly reviews, including whether they occur. DHS Privacy Office, *2017 Data Mining Report to Congress*, 22. Moreover, as risk assessments themselves have no accepted empirical basis, it is unlikely that these reviews could adequately address the core issues of the assessments' foundation or the validity of the factors used in the assessments. Additionally, risk assessments have been shown to disproportionately impact minorities in other settings, such as the criminal justice system. *See supra* text accompanying notes 57-60.

199 ATS also ingests and stores data from the Department of State's Consular Consolidated Database and Consular Electronic Application Center, TSA's Secure Flight Passenger Data, the FBI's Terrorist Screening Database, devices searched at the border, ICE's Student Exchange and Visitor Information System (SEVIS), and Passenger Name Records (PNR), among other sources. ATS 2017 PIA, 2-3, 39-41; PNR data can include name, ticket information, contact information, travel itinerary, billing information, and all historical changes to one's PNR. DHS, Privacy Impact Assessment for the Automated Targeting System, DHS/CBP/PIA-006(b), June 1, 2012 (hereinafter ATS 2012 PIA), 35, https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats006b_0.pdf. For more on ATS's role in electronic device border searches, *see supra* text accompanying notes 163-168; *see* also CBP Electronic Border Searches 2018 PIA, 10.

200 According to an October 3, 2018, addendum to the 2017 ATS PIA, CBP entered into a contract with a private database vendor to test and assess whether "ingestion of commercially available social media information" into ATS would aid CBP's work. CBP's stated goal, according to the privacy impact assessment, is to use social media information to better identify potential connections to known terrorist

propaganda channels and actors. Where there are matches or potential matches between social media handles and information already in ATS, CBP analysts conduct manual, directed queries and upload additional data into ATS, which may include social media information, in order to substantiate information linking an individual to terrorism or other suspicious activity. Once CBP incorporates the social media handles into a record in TECS, ATS, or AFI, it will be viewable to other users both internal and external to CBP. It is not clear what standards are used to identify matches and in what circumstances this information collection is occurring; in one instance, it is referred to as a "pilot." ATS 2017 PIA, "Addendum 3.3, ATS IntelCenter," 76-9. While the contracted vendor is not named in the addendum, ICE awarded a contract worth more than $800,000 to the data analytics company Giant Oak, Inc., on September 24, 2018, for "Open Source/Social Media Data Analytics for CBP." *See* ICE contracts with Giant Oak, Inc., September 24, 2018–September 24, 2019, USASpending, https://www.usaspending.gov/#/award/68790969. More information on Giant Oak and its DHS contracts can be found in the ICE section, *infra* text accompanying notes 353-359.

201 ATS applies its risk-based rules to domestic passengers as part of the joint CBP-TSA flight screening operation. *See* DHS Privacy Office, *2017 Data Mining Report to Congress*, 10; ATS 2017 PIA, 23; ATS-TSA PIA, Common Operating Picture, Phase II, 3-5. *See* also Electronic Privacy Information Center, "*EPIC v. CBP* (Analytical Framework for Intelligence)," https://epic.org/foia/dhs/cbp/afi/.

202 CBP uses ATS to nominate additional individuals for inclusion in the TSDB. ATS 2017 PIA, 25. The role of ATS in preflight and watch list screening is described in more detail in the TSA section; *see infra* text accompanying notes 258-297.

203 DHS Privacy Office, *2017 Data Mining Report to Congress*, 16; ATS 2017 PIA, 23; ATS-TSA PIA, Common Operating Picture, Phase II, 2-3. These assessments are also used to decide who gets permission to engage in trade across U.S. borders and, at the border, to decide who is allowed to enter the country and what level of questioning they must undergo. ATS 2017 PIA, 4.

204 CBP uses ATS risk assessments to determine whether further inspection of a person, shipment, or conveyance may be warranted, "even though an individual may not have been previously associated with a law enforcement action or otherwise be noted as a person of concern." ATS 2017 PIA, 4; ATS 2012 PIA, 19.

205 In assigning risk assessments, ATS incorporates information from many sources, including private contractors, the FBI's Terrorist Screening Database, and other government agencies. ATS 2017 PIA, 1, 10, 76.

206 ATS Final Rule, 5491.

207 ATS 2017 PIA, 8; Hearing on "Visa Overstays: A Gap in the Nation's Border Security" before the Subcommittee on Border and Maritime Security of the Committee on Homeland Security, House of Representatives, 115th Congress, May 23, 2017, No. 115-17 (hereinafter Congressional Hearing on Visa Overstays), 10, https://www.govinfo.gov/content/pkg/CHRG-115hhrg27610/pdf/CHRG-115hhrg27610.pdf.

208 ATS 2017 PIA, 8.

209 These analytical and data mining tools are provided by a facet of ATS, the Automated Targeting Initiative. DHS Privacy Office, *2017 Data Mining Report to Congress*, 16.

210 ATS 2017 PIA, 14, 43; DHS Privacy Office, Notice of Privacy Act System of Records, CBP–006 Automated Targeting System, System of Records, 77 Fed. Reg. 30297 (May 22, 2012), https://www.govinfo.gov/content/pkg/FR-2012-05-22/pdf/2012-12396.pdf.

211 ATS 2017 PIA, 14; ESTA 2016 PIA, 6.

212 For example, ICE, U.S. Coast Guard, and TSA personnel have direct access to ATS. ATS 2017 PIA, 5, 8. Personally identifiable information held in ATS can be shared outside DHS as long as personnel prepare a DHS-191 form to note the sharing of information. ATS 2012 PIA, 28. As an example of such dissemination of personal information, CBP passes photographs and certain personally identifiable information via ATS to the DHS Automated Biometric Identification System (IDENT), which is then forwarded to the FBI's Next Generation Identification (NGI) for comparison. ATS 2017 PIA, 17-19.

213 ATS 2017 PIA, 1.

214 Ibid.

215 Ibid., 35-37, 39-41, 46-47, 58-60.

216 DHS Privacy Office, *2017 Data Mining Report to Congress*, 16; ATS 2017 PIA, 1.

217 ATS 2017 PIA, 23. See *infra* text accompanying notes 277-297.

218 These tools also include statistical, geospatial, and temporal analysis capabilities. DHS, Privacy Impact Assessment for the DHS Data Framework, DHS/ALL/PIA-046, November 6, 2013 (hereinafter DHS Data Framework 2013 PIA), 13, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.

219 As of February 2018, data sets from at least 16 programs had been ingested into the DHS Data Framework, including CBP's ATS, ESTA, and border crossing information; ICE's SEVIS; TSA's Secure Flight; USCIS's index of A-Files relating to individuals who were victims of abuse or human trafficking; and USCIS and NPPD's Automated Biometric Identification System (IDENT). DHS, Privacy Impact Assessment for the DHS Data Framework, Appendix A, Approved Data Sets, DHS/ALL/PIA-046(b), February 14, 2018, 44, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-dhs-dataframeworkappendixa-february2018.pdf; DHS Privacy Office, *2017 Data Mining Report to Congress*, 46.

220 DHS, Privacy Impact Assessment for the DHS Data Framework, DHS/ALL/PIA-046(b), February 27, 2015, 3, https://www.dhs.gov/sites/default/files/publications/privacy-pia-046b-dhs-data-framework-20150227.pdf. The Data Framework includes two central repositories for data: Neptune and Cerberus. The previous practice was for the Data Framework to ingest unclassified information from DHS data systems into Neptune, which Neptune then stored and tagged. Once tagged, the unclassified data from Neptune was transferred to Cerberus, the classified "data lake" that DHS uses to perform classified searches of the unclassified data. Neptune tags data based on the type of data involved, the system from which the data originated, and when it was ingested into the Framework. DHS, Privacy Impact Assessment for the DHS Data Framework, DHS/ALL/PIA-046(a), August 29, 2014, 3, https://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-pia-046-a-dhs-data-framework-08292014.pdf. Cerberus is part of the "Top Secret/Sensitive Compartmented Information" domain. DHS, Privacy Impact Assessment Update for Neptune, DHS/ALL/PIA-046-1(b), February 27, 2015, 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-046-1-b-neptune-20150227.pdf.

221 Data Framework — Interim Process PIA, 8.

222 Specifically, the interim process was meant to expedite the identification of individuals "supporting the terrorist activities" of the Islamic State of Iraq and the Levant, al-Qa'ida in the Arabian Peninsula, the al-Nusrah Front, affiliated offshoots of these groups, or individuals seeking to join the Syria-Iraq conflict. Ibid., 1.

223 Ibid., 7.

224 DHS Privacy Office, *2017 Data Mining Report to Congress*, 46. *See* also DHS Privacy Office, *2016 Data Mining Report to Congress*, April 2017, 57, https://www.dhs.gov/sites/default/files/publications/2016%20Data%20Mining%20Report%20FINAL.pdf.

225 ATS 2017 PIA, 14.

226 Cantú and Joseph, "Trump's Border Security May Search Your Social Media by 'Tone.'"

227 For instance, the Defense Department uses a tone analysis system developed by IBM that purports to be able to interpret and visualize emotional styles and moods from Twitter time lines. Ibid. *See* also Jian Zhao et al., "PEARL: An Interactive Visual Analytic Tool for Understanding Personal Emotion Style Derived From Social Media," *Proceedings of the IEEE Symposium on Visual Analytics Science*

and Technology (2014): 203-212, https://ieeexplore.ieee.org/document/7042496.

228 *See*, for instance, Ahmed Abbasi, Ammar Hassan, and Milan Dhar, "Benchmarking Twitter Sentiment Analysis Tools" (finding that the best-performing sentiment analysis tools attain overall accuracy levels between 65 percent and 71 percent, with many low-performing tools yielding accuracies below 50 percent); Asaf Beasley, Winter Mason, and Eliot Smith, "Inferring Emotions and Self-Relevant Domains in Social Media: Challenges and Future Directions," *Translational Issues in Psychological Science* 2, no. 3 (2016): 238-247, https://psycnet.apa.org/record/2016-47442-004 (noting that social media posts containing sentiment only weakly predict users' self-reported measure of emotion); Asaf Beasley and Winter Mason, "Emotional States vs. Emotional Words in Social Media," *Proceedings of the Association for Computing Machinery Web Science Conference* (2015), https://dl.acm.org/citation.cfm?id=2786473 (noting that sentiment analysis tools are not sufficient to infer how users feel).

229 Siaw Ling Lo et al., "Multilingual Sentiment Analysis: From Formal to Informal and Scarce Resource Languages," *Artificial Intelligence Review* 48, no. 4 (2017): 515, 518 https://sentic.net/multilingual-sentiment-analysis.pdf (noting that most of the sentiment analysis studies to date have utilized lexicons and corpora in "proper English"). *See also* Duarte,Llanso, and Loup, *Mixed Messages?*, 14-15.

230 DHS, Privacy Impact Assessment for DHS Data Framework, Appendix C — Approved Users, DHS/ALL/PIA-046(b), September 2018, 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhswide-dhsdataframeworkappendixc-september2018.pdf.

231 DHS, Privacy Impact Assessment Update for the DHS Data Framework — External Sharing, DHS/ALL/PIA-046(c), March 30, 2016, 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-data%20framework-march2016%20%28003%29.pdf.

232 DHS Privacy Office, Notice of New Privacy Act System of Records, CBP–024 Intelligence Records System (CIRS) System of Records, 82 Fed. Reg. 44198 (September 21, 2017) (hereinafter CIRS SORN), https://www.federalregister.gov/d/2017-19718.

233 Ibid., 44201. Social media information collected by CBP for "situational awareness" activities is also likely stored in CIRS. DHS, Privacy Impact Assessment for the Publicly Available Social Media Monitoring and Situational Awareness Initiative, DHS/CBP/PIA-058, March 25, 2019, 6, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp58-socialmedia-march2019.pdf.

234 DHS, Final Rule, CBP–024 CBP Intelligence Records System (CIRS) System of Records, 83 Fed. Reg. 66557 (December 27, 2018) https://www.govinfo.gov/content/pkg/FR-2018-12-27/pdf/2018-27944.pdf.

235 Ibid.

236 CIRS SORN, 44199. In addition to ATS and CIRS, AFI also ingests CBP's ESTA and ICE's Student and Exchange Visitor System. AFI 2016 PIA, 3-4. It is unclear how specifically information from CIRS is transmitted to AFI — whether CIRS data is routinely uploaded into AFI or specific CIRS data sets are copied ad hoc for analysis in AFI.

237 AFI 2016 PIA, 1; AFI 2012 PIA, 1, 4; CBP, *Performance and Accountability Report Fiscal Year 2014*, 26, https://www.cbp.gov/sites/default/files/documents/CBP_DHS_2014%20PAR_508C.PDF. Other AFI analytic capabilities include creating an index of data in existing DHS systems, carrying out geospatial and temporal analysis, and performing federated queries against external data sources including the Department of State, the FBI, and commercial data aggregators. Federated or universal queries allow users to search data across many different databases and systems to provide a consolidated view of data about a person or entity. ATS 2017 PIA, 1. AFI also includes capabilities for detecting trends, patterns, and emerging threats, but little is known about the underlying data AFI users have access to in conducting those types of analyses. DHS Privacy Office, *2017 Data Mining Report to Congress*, 26.

238 *See Electronic Privacy Information Center v. U.S. Customs and Border Protection*, 2015 WL 12434257 (D.D.C.), https://epic.org/foia/dhs/cbp/afi/20.1-EPIC-MSJ-MPA.pdf.

239 The only criterion that AFI users must meet to upload internet sources is that they believe the information is relevant to a project. AFI 2012 PIA, 9; AFI 2016 PIA, 4n19; DHS Privacy Office, Notice of Privacy Act System of Records, DHS/CBP–017 Analytical Framework for Intelligence (AFI) System of Records, 77 Fed. Reg. 33753 (June 7, 2012) (hereinafter AFI SORN), https://www.govinfo.gov/content/pkg/FR-2012-06-07/html/2012-13813.htm.

240 Information in AFI can include "information from any source including public and commercial sources, which may be relevant." AFI SORN. Publicly available sources are stored even if "the accuracy of information obtained or introduced occasionally may be unclear." AFI Final Rule, 47768.

241 For the full list of data sources available through AFI, *See* AFI 2016 PIA, Appendix B, updated November 30, 2018, 23-29. Starting in September 2016, AFI began copying the volumes of information it accesses into its own servers. AFI 2016 PIA, 2-3. AFI now uses an open-source platform designed by Palantir that requires AFI to store multiple copies of data within the platform. This platform provides for shared storage and analysis by replicating the underlying data sources and storing the replicated data in multiple places. This open-source platform model, DHS acknowledged, "presents privacy challenges as its functionality relies on continuous replication of data." Ibid.

242 AFI 2016 PIA, 4. The difference between AFI "projects" and "products" is that the former involve "in progress" research and analysis that may or may not lead to a finished intelligence product. DHS, Privacy Compliance Review of the U.S. Customs and Border Protection (CBP) Analytical Framework for Intelligence (AFI), December 19, 2014, 2, 6, https://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-afi-12-19-2014.pdf.

243 Sam Biddle, "How Peter Thiel's Palantir Helped the NSA Spy on the Whole World," *Intercept*, February 22, 2017, https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/.

244 Spencer Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine"; Spencer Woodman, "Documents Suggest Palantir Could Help Power Trump's 'Extreme Vetting' of Immigrants," *Verge*, December 21, 2016, https://www.theverge.com/2016/12/21/14012534/palantir-peter-thiel-trump-immigrant-extreme-vetting.

245 CBP, "Analytical Framework for Intelligence Operational Status & Security," https://epic.org/foia/dhs/cbp/afi/14-04-08-CBP-FOIA-20150205-Production-p4.pdf#page=8.

246 Sam Biddle, "How Peter Thiel's Palantir Helped the NSA Spy on the Whole World."

247 Peter Waldman, Lizette Chapman, and Jordan Robertson, "Palantir Knows Everything About You," *Bloomberg BusinessWeek*, April 19, 2018, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.

248 Ibid. (noting that after the departure of several JP Morgan executives who had taken advantage of Palantir's capabilities, the bank "drastically curtailed its Palantir use, in part because 'it never lived up to its promised potential'").

249 AFI Final Rule, 66558.

250 CBP, "AFI Analyst Training," https://epic.org/foia/dhs/cbp/afi/14-04-08-CBP-FOIA-20150205-Production-p4.pdf#page=219. *See infra* text accompanying notes 414-417.

251 DHS contract with Thundercat Technology, LLC, September 21, 2017–September 20, 2018, USASpending, https://www.usaspending.gov/#/award/23784019; DHS contract with Panamerica Computers, Inc., for Babel Software Licenses, September 21, 2018–September 20, 2019, USASpending, https://www.usaspending.gov/#/award/68617237; CBP contract with Thundercat Technology, LLC, September 21, 2016–September 20, 2017, USASpending, https://www.usaspending.gov/#/award/23781451; CBP contract with Thundercat Technology, LLC, September 21, 2015–September 20, 2016,

USASpending, https://www.usaspending.gov/#/award/23779146; Office of Inspector General, DHS, *Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence*, September 2, 2015, 2, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-137-Sep15.pdf (noting that the Targeting and Analysis Systems Program Directorate administers and manages AFI).

252 Babel Street, "How It's Done," https://www.babelstreet.com/#about.

253 Curtis Waltman, "Meet Babel Street, the Powerful Social Media Surveillance Used by Police, Secret Service, and Sports Stadiums," *Motherboard*, April 17, 2017, https://motherboard.vice.com/en_us/article/gv7g3m/meet-babel-street-the-powerful-social-media-surveillance-used-by-police-secret-service-and-sports-stadiums.

254 Ibid.; Babel Street, "Babel X," https://www.babelstreet.com/. While the *Washington Post* reported in 2017 that Babel Street does not access individuals' Facebook profiles, it is not clear whether that is still the case and what kinds of Facebook information Babel Street technologies currently collect. Aaron Gregg, "For This Company, Online Surveillance Leads to Profit in Washington's Suburbs," *Washington Post*, September 10, 2017, https://www.washingtonpost.com/business/economy/for-this-company-online-surveillance-leads-to-profit-in-washingtons-suburbs/2017/09/08/6067c924-9409-11e7-89fa-bb822a46da5b_story.html?utm_term=.4f7b99fd5135.

255 DHS Privacy Office, *2017 Data Mining Report to Congress*, 16; DHS Data Framework 2013 PIA, 13.

256 *See*, for example, Waldman, Chapman, and Robertson, "Palantir Knows Everything About You"; Angel Diaz and Rachel Levinson-Waldman, "Hold Private Police Partners Accountable, Too: For-Profit Companies Are Making Millions With Special Access to NYPD Information," *Daily News*, October 26, 2018, http://www.nydailynews.com/opinion/ny-oped-hold-private-police-partners-accountable-too-20181025-story.html.

257 Aviation and Transportation Security Act, 49 U.S.C. § 114(d).

258 ATS 2017 PIA, 22-23.

259 *See*, for example, Center for Constitutional Rights, "Leaked Guidelines for Placement on No-Fly List Show System Ripe for Abuse," July 24, 2014, https://ccrjustice.org/home/press-center/press-releases/leaked-guidelines-placement-no-fly-list-show-system-ripe-abuse; *El Ali et al*., No. 8:18-cv-02415-PX; David Smith, " 'The Illusion of Security': No-Fly List Draws Scrutiny From Left and Right," *The Guardian*, December 9, 2015, https://www.theguardian.com/us-news/2015/dec/09/no-fly-list-errors-gun-control-obama.

260 DHS, "DHS Transition Issue Paper: Enhancing International Aviation Security," in *Strategic Issue Paper Summaries*, 28.

261 Hearing on "Secure Flight: Additional Actions Needed to Determine Program Effectiveness and Strengthen Privacy Oversight Mechanisms" before the Subcommittee on Transportation Security, House Committee on Homeland Security, House of Representatives, 113th Congress, September 18, 2014 (statement of Jennifer Grover, acting director, Homeland Security and Justice), 1, https://www.gao.gov/assets/670/665884.pdf.

262 Office of Inspector General, DHS, *Implementation and Coordination of TSA's Secure Flight Program*, OIG-12-94, July 2012, 23, https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf. Scores must meet a minimum threshold to be considered a potential match, but it is not clear what that threshold is, raising concerns about whether the system is sufficiently rigorous. Ibid.

263 DHS, Privacy Impact Assessment Update for Secure Flight, DHS/TSA/PIA-018(f), September 4, 2013, 5, https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-secure-flight-update-09042013.pdf.

264 ATS-TSA PIA, Common Operating Picture, Phase II, 3.

265 DHS, Privacy Impact Assessment for Secure Flight, DHS/TSA/PIA-018(h), July 12, 2017 (hereinafter Secure Flight 2017 PIA), 1-2, https://www.dhs.gov/sites/default/files/publications/pia_tsa_secureflight_18%28h%29_july2017.pdf. CBP also uses the Centers for Disease Control and Prevention's Do Not Board List for Secure Flight. Ibid., 2n4.

266 *See* National Counterterrorism Center, "Watchlisting Guidance," March 2013, 10, https://www.eff.org/files/2014/07/24/2013-watchlist-guidance_1.pdf; Jeremy Scahill and Ryan Devereaux, "The Secret Government Rulebook for Labeling You a Terrorist," *Intercept*, July 23, 2014, https://theintercept.com/2014/07/23/blacklisted/; Center for Constitutional Rights, "Leaked Guidelines for Placement on No-Fly List."

267 DHS, Privacy Impact Assessment Update for the Watchlist Service, DHS/ALL-027(e), May 5, 2016, 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-027-E-uscis-wlsfdnsds-may2016.pdf. *See* also Jerome P. Bjelopera, Bart Elias, and Alison Siskin, *The Terrorist Screening Database and Preventing Terrorist Travel*, Congressional Research Service, 7-5700, November 7, 2016, 1, https://fas.org/sgp/crs/terror/R44678.pdf.

268 DHS, Use of the Terrorist Screening Database System of Records, 81 Fed. Reg. 3811 (January 22, 2016) (hereinafter Use of TSDB SORN), https://www.gpo.gov/fdsys/pkg/FR-2016-01-22/pdf/2016-01167.pdf.

269 National Counterterrorism Center, "Watchlisting Guidance," 10. This guidance also specifies that a posting on a social media site "should not automatically be discounted merely because of the manner in which it was received. Instead, the nominating agency should evaluate the credibility of the source, as well as the nature and specificity of the information, and nominate even if that source is uncorroborated." Ibid., 34. CBP is one such agency that submits watch list nominations. ATS 2017 PIA, 25. In fiscal year 2016, CBP nominated more than 3,400 individuals to the Terrorist Screening Database. DHS, "DHS Transition Issue Paper: Travel Security and Facilitation," in *Strategic Issue Paper Summaries*, 216. A nomination is accepted to the TSDB if the Terrorist Screening Center determines that the information meets a reasonable-suspicion standard and there is sufficient identifying information. Bjelopera, Elias, and Siskin, *The Terrorist Screening Database and Preventing Terrorist Travel*, 5.

270 Office of Senator Dianne Feinstein, "Findings From Joint Response From the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI) to Congressional Questions Regarding the Terrorist Identities Datamart Environment (TIDE) and the Terrorist Screening Database (TSDB)," 2016, https://www.feinstein.senate.gov/public/_cache/files/f/b/fb745343-1dbb-4802-a866-cfdfa300a5ad/BCD664419E5B375C638A0F250B37DCB2.nctc-tsc-numbers-to-congress-06172016-nctc-tsc-final.pdf. *See* also Jeremy Scahill and Ryan Devereaux, "Watch Commander: Barack Obama's Secret Terrorist-Tracking System, by the Numbers," *Intercept*, August 5, 2014, https://theintercept.com/2014/08/05/watch-commander/ (noting that, as of 2013, 680,000 names were in the TSDB, including those of 5,000 Americans).

271 *See*, for example, *El Ali et al*., No. 8:18-cv-02415-PX; *Latif v. Holder*, 28 F. Supp. 3d 1134 (D. Or. 2014); *Tarhuni v. Sessions,* No. 3:13-CV-00001-BR, 2018 WL 3614192 (D. Or. July 27, 2018); National Counterterrorism Center, "Watchlisting Guidance," 37-42. In 2016, DHS revised the Watchlist Service System of Records Notice (SORN) to further expand the categories of individuals covered by the system. The revised SORN explicitly includes those who "do not otherwise satisfy the requirements for inclusion in the TSDB" but (1) are relatives, associates, or others closely connected with a known or suspected terrorist, (2) "were officially detained during military operations, but not as enemy prisoners of war, and who have been identified as possibly posing a threat to national security," or (3) are known or suspected to be or have been engaged in conduct constituting, in aid of, or related to transnational organized crime. Use of TSDB SORN; DHS, Privacy Impact Assessment for ICE Investigative Case Management, DHS/ICE/PIA-045, June 16, 2016 (hereinafter ICM 2016 PIA), 18, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.

272 The No Fly List includes those who are not allowed to board a commercial aircraft flying into, out of, over, or within U.S. airspace,

or point-to-point international flights operated by U.S. carriers. The Selectee List includes those who must undergo extra screening before boarding a commercial aircraft. Office of Inspector General, *Implementation and Coordination of TSA's Secure Flight Program*, 2. For a discussion of the overbroad standards of these lists, *see* Center for Constitutional Rights, "Leaked Guidelines for Placement on No-Fly List"; Scahill and Devereaux, "The Secret Government Rulebook for Labeling You a Terrorist."

273 In the case of Rahinah Ibrahim, a Malaysian national working toward her Ph.D. at Stanford, it took nine years of litigation before her name was cleared. A January 2019 ruling in the Ninth Circuit found that even after the government determined that Ibrahim did not pose a threat to national security, the government engaged in years of "scorched earth litigation," refusing to allow Ibrahim to return to the United States. *Ibrahim v. U.S. Department of Homeland Security*, No. 14-16161, 2019 WL 73988, at 17 (9th Cir., Jan. 2, 2019). The en banc Ninth Circuit found that there was considerable evidence indicating that the Justice Department attorneys had acted in "bad faith" and that Ibrahim was entitled to full attorneys' fees under the Equal Access to Justice Act. *See* also "The FBI Checked the Wrong Box and a Woman Ended Up on the Terrorism Watch List for Years," *ProPublica*, December 15, 2015, https://www.propublica.org/article/fbi-checked-wrong-box-rahinah-ibrahim-terrorism-watch-list. *See* also *Latif v. Holder*, 28 F. Supp. 3d 1134; *Tanvir v. Lynch,* 128 F. Supp. 3d 756 (S.D.N.Y. 2015) (noting that DHS lacks "a meaningful mechanism for travelers who have been denied boarding to correct erroneous information in the government's terrorism databases").

274 Nominations to a TSA Watch List may come from within TSA, from other DHS components, or from other government agencies, and those nominations may be informed by social media. Secure Flight 2017 PIA, 3-4. *See*, for example, Susan Hasman, director of security operations coordination to federal security directors, "400.5 — ROUTINE — OD-400-19-12 — TSA Watch List (Security Notification)," March 19, 2018, https://www.justsecurity.org/wp-content/uploads/2018/05/watch-list_scan.pdf (noting that individuals who are "publicly notorious" can be nominated to the TSA Watch List).

275 Secure Flight 2017 PIA, 6. The TSA Watch List explicitly includes those "who are not on a TSDB watch list but who nonetheless present a threat to transportation or national security." Ibid., 4. TSA retains the master files of the lists for 30 years. Ibid., 9.

276 Hasman, "400.5 — ROUTINE — OD-400-19-12 — TSA Watch List (Security Notification)." *See* Faiza Patel, "Does TSA Really Need a Watch List for 'Unruly' Travelers?" Just Security, May 23, 2018, https://www.justsecurity.org/56631/tsa-explain-unruly-passengers-watch-list/.

277 These international flights include incoming international flights, flights that fly over the United States but do not touch down, and flights on U.S. carriers that fly from one international point to another international point (point-to-point flights); it is not clear whether outgoing international flights are also prescreened by ATS. ATS 2017 PIA, 23.

278 ATS 2017 PIA, 23; Secure Flight 2017 PIA, 2. CBP also receives information from TSA about possible and confirmed watch list matches for individuals on international flights of covered U.S. aircraft operators, which it also compares against ATS records. DHS, Privacy Impact Assessment Update for the ATS-TSA/CBP Common Operating Picture Program, DHS/CBP/PIA-006(c), January 31, 2014, 5, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-atsupdate-01312014_0.pdf.

279 DHS Privacy Office, *2017 Data Mining Report to Congress*, 18. When an individual matches with information or rules in ATS, the match leads either to further inspection action or to a recommendation to carriers not to allow such persons to board. Ibid., 19.

280 ATS 2017 PIA, 23.

281 DHS, Privacy Impact Assessment Update for Secure Flight Silent Partner and Quiet Skies, DHS/TSA/PIA-018(i), April 19, 2019 (hereinafter Silent Partner and Quiet Skies 2019 PIA), 2, https://www.dhs.gov/sites/default/files/publications/pia-tsa-spqs018i-april2019_1.pdf.

282 Jana Winter, "Welcome to the Quiet Skies," *Boston Globe*, July 28, 2018, http://apps.bostonglobe.com/news/nation/graphics/2018/07/tsa-quiet-skies/?p1=HP_SpecialTSA.

283 Jana Winter and Jenn Abelson, "TSA says it no longer tracks regular travelers as if they may be terrorists," *Boston Globe*, December 15, 2018, https://www2.bostonglobe.com/news/nation/2018/12/15/curtails-quiet-skies-passenger-surveillance/2IRAv2AwjGpUcgq08mHaPM/story.html.

284 Silent Partner and Quiet Skies 2019 PIA, 2.

285 Ibid. The rules TSA shares with ATS to designate individuals for the Quiet Skies List "must pertain to a specific potential threat to aviation security within the Homeland, as assessed by TSA." Ibid., 3 n7. In contrast, the Silent Partner rules are broader and "must pertain to a specific potential threat to aviation security *or* the Homeland" (emphasis added). Ibid., 3n7.

286 Ibid., 3.

287 Ibid., 2.

288 Ibid., 11-12; ATS 2017 PIA, 27. For "Inhibited Passengers" identified by TSA and shared with ATS, ATS screens those records against its holdings and against lists like the TSDB. ATS identifies "possible watchlist matches who are subsequently cleared," which are then retained in ATS for seven years. Confirmed matches to a watch list record are retained in ATS for 15 years, and in Secure Flight for 99 years. Secure Flight information that is linked to a border security, national security, significant health risk, or counterterrorism matter is retained in ATS for the life of the matter. Ibid., 27.

289 Individuals who are flagged in ATS as "high risk" are not provided notice of their flagging as ATS does not collect information from individuals directly and DHS has exempted many parts of ATS from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. *See* ATS Final Rule. The ATS privacy impact assessments state that those who would like to contest or correct any information in ATS can contact the CBP Information Center or DHS Traveler Redress Inquiry Program. For instance, travelers may obtain access to their Passenger Name Record (PNR) data in ATS, but not to the results of any ATS rules or analyses applied to their PNR data. ATS 2012 PIA, 29-30.

290 TSA and CBP have a broad arrangement through which they share information, which may include social media information, about watch-listed travelers and their traveling companions. All information on TSA-identified and CBP-identified "Inhibited Passengers" is easily accessible to both TSA and CBP via a shared dashboard display. ATS-TSA PIA, Common Operating Picture, Phase II, 3.

291 Ibid., 4-5.

292 Ibid., 8.

293 The shared dashboard display is viewable at CBP's National Targeting Center and TSA's Operations Center. Ibid., 2-3. CBP also displays visa denials and revocations, information on lost or stolen passports, and ESTA denial data on the common dashboard. Ibid., 5.

294 Ibid., 8.

295 ATS 2017 PIA, 8, 9n7. Other DHS components, including ICE and Border Patrol, also use ATS-P and the mobile app for "decision-support." Ibid., 8.

296 Ibid., 8. DHS personnel use ATS-P to "focus efforts on potentially high-risk passengers by eliminating labor-intensive manual reviews of traveler information." Ibid. It is not clear what these "uniform and user-defined rules" are or how DHS ensures that they are valid and free from bias. For ATS's "risk-based rules" in general, CBP, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the DHS Office of the General Counsel are supposed to conduct joint quarterly reviews of the rules. DHS Privacy Office, *2017 Data Mining Report to Congress*, 22.

297 ATS 2017 PIA, 8-9. ATS-P received a technology refresh, UPAX, to more succinctly display query results across multiple source systems, as well as "integrat[e] risk assessment and case manage-

ment functionality with the presentation of query results." Ibid., 10. This may suggest that users, including non-CBP users, would be able to view travelers' risk assessments through ATS-P and the mobile application.

298 Privacy Impact Assessment for the TSA PreCheck Application Program, DHS/TSA/PIA-041, September 4, 2013 (hereinafter PreCheck 2013 PIA), 1, https://www.dhs.gov/sites/default/files/publications/privacy_pia_041_tsa%20precheck%20application%20program_september%202013_0.pdf.

299 Government Accountability Office, Report to Congressional Requesters, *Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness*, September 2014, 15-16, https://www.gao.gov/assets/670/665676.pdf.

300 *See* "CBP Trusted Traveler and Trusted Worker Populations," ATS 2017 PIA, 30.

301 Agreement Relating to TSA PreCheck Application Expansion, HSTS02-15-H-OIA037X, https://s3.amazonaws.com/s3.documentcloud.org/documents/1508090/ota-articles-for-pre-check-application-expansion.pdf.

302 *See*, for example, Joe Sharkey, "PreCheck Expansion Plan Raises Privacy Concerns," *New York Times*, March 9, 2015, https://www.nytimes.com/2015/03/10/business/precheck-expansion-plan-raises-privacy-concerns.html; Amber Corrin, "TSA Pulls Back on Big-Data PreCheck Expansion," *Federal Times*, February 16, 2015, https://www.federaltimes.com/management/2015/02/16/tsa-pulls-back-on-big-data-precheck-expansion/.

303 "Special Notice Posting for the PreCheck Application Expansion," Solicitation HSTS02-15-R-OIA037, Federal Business Opportunities, February 7, 2015, https://www.fbo.gov/utils/view?id=d883f342353397d6ee9b5630d418c973. The TSA's PreCheck privacy impact assessment from January 2016 reaffirms its interest in having private-sector entities "perform identity assurance and criminal history assessments" using commercial and publicly available data, though the document does not indicate that social media data will be used. DHS, Privacy Impact Assessment Update for the TSA PreCheck Application Program, DHS/TSA/PIA-041(a), January 22, 2016 (hereinafter PreCheck 2016 PIA), 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-041-a-tsa%20precheck%20application%20program-february2016.pdf.

304 DHS Universal Enrollment Services Contract with Idemia Identity & Security USA LLC, USASpending, September 1, 2017–September 4, 2019, https://www.usaspending.gov/#/award/24290264.

305 TSA, "Justification for Other Than Full and Open Competition," J&A Universal Enrollment Services (UES) Bridge Contract Modification, Solicitation Number 70T02018R9NOIA248, Federal Business Opportunities, September 18, 2018, 2, https://www.fbo.gov/utils/view?id=7654f14c5beec3837347c03cfccee72c; *see* also TSA Office of Contracting and Procurement, Universal Enrollment Services (UES) Request for Proposals, Federal Business Opportunities, March 7, 2018, 112, https://www.fbo.gov/utils/view?id=7631ca3cab726e4097c2dd5fa8e17668; Universal Enrollment Services (UES) Notice of Intent to Sole Source, *GovTribe*, May 1, 2018, https://govtribe.com/opportunity/federal-contract-opportunity/universal-enrollment-services-ues-notice-of-intent-to-sole-source-70t02018r9noia248.

306 TSA, "Justification for Other Than Full and Open Competition"; "Big Data," Idemia, accessed December 28, 2018, https://www.morpho.com/en/big-data. Idemia "has been building and managing databases of entire populations for governments, law enforcement agencies and other government bodies around the world, whether for national ID, health cards, bank cards or even driver license programs." Ibid. Idemia, formerly MorphoTrust, LLC, was alleged to have embedded Russian-made code purchased from a Kremlin-connected firm into software that it sold to the FBI for its fingerprint-recognition technology, raising concerns that Russian hackers could compromise law enforcement computer systems. Chris Hamby, "FBI Software for Analyzing Fingerprints Contains Russian-Made Code, Whistleblowers Say," *Buzzfeed News*, December 26, 2017, https://www.buzzfeednews.com/article/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a.

307 ICE, "Who We Are," https://www.ice.gov/about. The secretary of DHS delegated ICE's investigative authority, pursuant to the Homeland Security Act of 2002, to ICE in DHS, "Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement," Delegation Number 7030.2, November 13, 2004, https://www.hsdl.org/?abstract&did=234774.

308 *See*, for example, Sarah Ruiz-Grossman, "ICE Dramatically Increased Workplace Arrests of Undocumented Immigrants in 2018," *Huffington Post*, December 12, 2018, https://www.huffingtonpost.com/entry/ice-immigration-arrests-work-undocumented-immigrants_us_5c105b3fe4b0ac537179c247; Maria Sacchetti and David Weigel, "ICE Has Detained or Deported Prominent Immigration Activists," *Washington Post*, January 19, 2018, https://www.washingtonpost.com/powerpost/ice-has-detained-or-deported-foreigners-who-are-also-immigration-activists/2018/01/19/377af23a-fc95-11e7-a46b-a3614530bd87_story.html?utm_term=.ed71c0e7a6e1; Alanna Durkin Richer, "Ex-judges to ICE: End Immigration Arrests at Courthouses," *Associated Press*, December 12, 2018, https://www.apnews.com/e401e85400ee44ab9dd51ace042be399.

309 ICE, "HSI Special Agent Brochure," February 2011, https://www.ice.gov/doclib/careers/pdf/investigator-brochure.pdf; ICE, "Enforcement and Removal Operations," https://www.ice.gov/ero.

310 DOJ Offices of the United States Attorneys, Federal Investigative Agencies, https://www.justice.gov/usao-mdpa/federal-investigative-agencies.

311 *See*, for example, ICM 2016 PIA, 18.

312 Ibid., 22.

313 Ibid., 18.

314 Ibid. ICE limits collection of publicly available information to "credible, industry-wide sources" but offers no information about those sources or how they are chosen. Ibid., 21-22.

315 Undercover agents may also be granted access to a restricted site in certain circumstances. Ibid., 18. There are no publicly available criteria or standards for when ICE can initiate an undercover operation. However, a leaked handbook outlines some factors that managers should take into consideration when assessing the need for an undercover operation, such as "risk of civil liability or other loss to the U.S. Government." *See* ICE Office of Investigations, *Undercover Operations Handbook*, OI HB 08-04, April 14, 2008, 39, https://www.unicornriot.ninja/wp-content/uploads/2018/06/ice-undercover-operations.pdf#page=50.

316 ICM 2016 PIA, 2. Before entering any new information, agents and support personnel are trained to compare it with information already in the system and external investigative case files, and subject records and case documents must be reviewed and approved by a supervisor before they can become "available for use" in an investigation. Audit logs capture all user activity, but it is not known how, or whether, these logs are reviewed. Ibid., 5, 21.

317 Ibid., 6. From ICM, users can query CBP's ATS and manually copy data into ICM. Ibid., 17.

318 Ibid., 29-30.

319 *See* National Immigration Law Center, *Untangling the Immigration Enforcement Web*, September 2017, 3, https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf.

320 ICM 2016 PIA, 30; ICE, "Law Enforcement Information Sharing Initiative," https://www.ice.gov/le-information-sharing. For more on "subject records," *see* DHS, Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing, December 22, 2010, 2-3, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf.

321 Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine." Electronic Privacy Information Center, FOIA Request Letter to Catrina Pavlik-Keenan, FOIA officer, ICE, August

14, 2017, 1-2, https://epic.org/foia/palantir/EPIC-17-08-10-ICE-20170810-Request.pdf.

322 ICE contract with Palantir USG, Inc., September 26, 2014–September 25, 2019, USASpending, https://www.usaspending.gov/#/award/68924715.

323 Contract Award Notice, ICE Investigative Case Management System, Solicitation Number HSCETC-14-R-00002, *Federal Business Opportunities,* https://www.fbo.gov/spg/DHS/INS/ICE-OAQ-TC/HSCETC-14-R-00002/listing.html. *See* also ICM 2016 PIA, 23-24.

324 Chantal Da Silva, "ICE Just Launched a $2.4M Contract With a Secretive Data Surveillance Company That Tracks You in Real Time," *Newsweek*, June 7, 2018, https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493.

325 Ibid.

326 DHS, "Justification and Approval for Other Than Full and Open Competition."

327 PenLink, "XNET: Investigating Beyond Phone Calls," https://www.penlink.com/xnet/.

328 ICE/HSI contract with West Publishing Corporation, January 19, 2017–October 31, 2021, Federal Procurement Data System — Next Generation, https://assets.documentcloud.org/documents/4546854/TR-Attachment-1.pdf.

329 Thomson Reuters, CLEAR Brochure, "The Smarter Way to Get Your Investigative Facts Straight," 2, 6, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf.

330 ICE Office of Acquisition Management, Investigations & Operations Support Dallas, "Limited Source Justification — Consolidated Lead Evaluation and Reporting (CLEAR)," 2, https://www.mediafire.com/file/y2e3vk65z6v3k6x/LSJ_Final.pdf.

331 Ibid.; FALCON-SA 2016 PIA, 35. *See* also Homeland Security Investigations Mission Support, "FALCON Operations & Maintenance Support & System Enhancement, Performance Work Statement," May 11, 2015, 16, https://www.ice.gov/doclib/foia/contracts/palantirTechHSCETC15C00001.pdf.

332 *See*, for example, Congressional Hearing on Visa Overstays, 2, 13; Office of Inspector General, DHS, *DHS Tracking of Visa Overstays Is Hindered by Insufficient Technology,* OIG-17-56, May 1, 2017 (hereinafter OIG May 2017 Visa Overstay Tracking Report), 1, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-56-May17_0.pdf.

333 OIG May 2017 Visa Overstay Tracking Report, 1.

334 Alex Nowrasteh, "Terrorists by Immigration Status and Nationality: A Risk Analysis, 1975-2017."

335 DHS, *Fiscal Year 2017 Entry/Exit Overstay Report,* 11, 18, https://www.dhs.gov/sites/default/files/publications/18_1009_S1_Entry-Exit-Overstay_Report.pdf.

336 Congressional Hearing on Visa Overstays, 10; ATS 2017 PIA, 8. ICE's LeadTrac system stores the information, including from social media, collected by the programs and initiatives described in this section. According to the LeadTrac privacy impact assessment, information from social media can be copied and pasted or summarized in a LeadTrac subject record. DHS, Privacy Impact Assessment for LeadTrac System, DHS/ICE/PIA-044, July 22, 2016 (hereinafter LeadTrac 2016 PIA), 11, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-leadtrac-july2016.pdf. According to the LeadTrac SORN, the system contains information not only on the target individual, but also on his or her associates (e.g., family members and employers of suspected status violators) who may be legal permanent residents or U.S. citizens. LeadTrac SORN, *supra* note 78, 52700.

337 LeadTrac 2016 PIA, 1, 9-10.

338 DHS, "DHS Transition Issue Paper: Counterterrorism," 6, in *Strategic Issue Paper Summaries.*

339 OIG May 2017 Visa Overstay Tracking Report, 8, 16.

340 Congressional Hearing on Visa Overstays, 13. According to the December 2016 issue of *SEVP Spotlight*, the Student Exchange and Visitor Program newsletter, this team also helps identify students or schools suspected of violation. HSI, *SEVP Spotlight* 6, no. 4 (December 2016): 3, https://studyinthestates.dhs.gov/assets/sevp_spotlight_december_2016_final.pdf.

341 The three "success stories" listed are "HSI Los Angeles Arrest of a Jordanian National in November 2014"; "HSI New York AWOL Case of a Yemen National in January 2015"; and "HSI San Diego Request for Open-Source Intelligence Report of Saudi Arabia National in May 2015." The descriptions for each are entirely redacted. DHS, "CTCEU Open Source Team Success Stories," https://www.brennancenter.org/sites/default/files/analysis/ICE%20FOIA%20Social%20Media%20Pilot%20Programs%20-%20BCJ.pdf#page=8.

342 *See* Congressional Hearing on Visa Overstays, 13.

343 A "sensitive" field is one "related to a sensitive technology on the DOS Technology Alert List." DHS, "Visa Overstay Enforcement Investigations Expenditure Plan," *Fiscal Year 2016 Report to Congress*, August 1, 2016, 4, https://www.dhs.gov/sites/default/files/publications/Immigration%20and%20Customs%20Enforcement%20-%20Visa%20Overstay%20Enforcement%20Investigations%20Expenditure%20Plan.pdf; Department of State, "Using the Technology Alert List (Update)," August 1, 2002, https://www.nafsa.org/uploadedFiles/dos_cable_provides_update.pdf?n=1034.

344 DHS, "Visa Overstay Enforcement Investigations Expenditure Plan," 5-6.

345 The program is unnamed in the Inspector General report but referred to in several reports and testimonies as the "Overstay Lifecycle pilot." In documents obtained by the Brennan Center via FOIA it is sometimes referred to as the "Visa Security Social Media Pilot Program." It is possible that this discrepancy is due to the fact that two different parts of HSI implement this program — the Visa Security Program (which vets visas at certain State Department posts) and the Counterterrorism and Criminal Exploitations Unit (which investigates overstay leads). *See* HSI, National Security Investigations Division, "Visa Security Social Media Pilot Program," https://www.brennancenter.org/sites/default/files/analysis/ICE%20FOIA%20Social%20Media%20Pilot%20Programs%20-%20BCJ.pdf.

346 Office of Inspector General, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success,* 3-4.

347 Ibid., 3.

348 DHS, "Visa Overstay Enforcement Investigations Expenditure Plan," 3-4.

349 Ibid.

350 Ibid., 3.

351 Ibid.

352 The report noted that enabling this capability "will require enhancements to PATRIOT through third-party systems/program modifications." Ibid., 4. Part of the $5.295 million identified for "Information Technology, Social Media Exploitation, & Enhancements" in the expenditure plan for the report was allocated to "creating connectivity to bridge the PATRIOT database to private vendor social media software for real-time vetting during the pre-entry adjudication process and procuring associated equipment and services to execute the mission." Ibid., 6.

353 ICE contract with Giant Oak, Inc., "Open Source/Social Media Data Analytics — VSP," August 21, 2018–August 20, 2019, USASpending, https://www.usaspending.gov/#/award/67807277; ICE contract with Giant Oak, Inc., "Open Source/Social Media Data Analytics — CTCEU," June 13, 2018–August 31, 2019, USASpending, https://www.usaspending.gov/#/award/66685141.

354 ICE contracts with Giant Oak, Inc., September 4, 2014 — September 24, 2018, "Spending by Prime Award," USASpending, https://www.usaspending.gov/#/search/f2b8f8d69d8696753510a172f52d46ad. In September 2018, ICE contracted yet again with Giant

Oak for $806,836, but the description specifies "open-source/social media data analytics for CBP." It is not clear why ICE would designate its spending this way, rather than CBP contracting with the company itself. ICE contract with Giant Oak, Inc., "Open Source/Social Media Data Analytics for CBP," September 24, 2018–September 24, 2019, USASpending, https://www.usaspending.gov/#/award/68790969. One of ICE's contracts with Giant Oak extends to August 31, 2022. ICE contract with Giant Oak, Inc., "Open Source/Social Media Data Analytics," September 25, 2017–August 31, 2022, USASpending, https://www.usaspending.gov/#/award/23831407.

355 "Statement of Work," ICE Contract #HSCEMD-14-C-00002 P00007, 31.

356 Thomas Brewster, "Trump's Immigration Cops Just Spent $3 Million on These Ex-DARPA Social Media Data Miners," *Forbes*, September 27, 2017, https://www.forbes.com/sites/thomasbrewster/2017/09/27/trump-immigration-social-media-surveillance-giant-oak-penlink-palantir/#7a77a4933e3b.

357 "Statement of Work," ICE Contract #HSCEMD-14-C-00002 P00007, 33. The contract outlines various restrictions relating to obtaining information from social media sources. The contractor is only to use publicly accessible, unrestricted online sources; may not circumvent restrictions placed on system users; may not interact with individuals who posted the information; may not appropriate online identities; and must abide by safeguards for personally identifiable information outlined in DHS policy. Ibid., 34.

358 Ibid., 33.

359 Ibid., 35.

360 *See* sidebar "Automatic Extreme Vetting," accompanying notes i-vii.

361 Harwell and Miroff, "ICE Just Abandoned Its Dream of 'Extreme Vetting' Software."

362 Ibid.

363 The award of the contract to CRSA was protested by ManTech, another big data analytics company. The Government Accountability Office issued a recommendation in November 2018 that ICE reevaluate the price quotations submitted by SRA and ManTech and make a new selection decision. Government Accountability Office, "Matter of ManTech Advanced Systems International, Inc." file B-416734, November 27, 2018, https://www.gao.gov/assets/700/695802.pdf. On February 1, 2019, another protest was filed, by a company called Amyx. *See* G2Xchange, "Update: Protest of $113M DHS ICE Visa Lifecycle Vetting Operations Support BPA denied," April 15, 2019, https://etc.g2xchange.com/statics/gao-sides-with-protester-on-113m-dhs-ice-visa-lifecycle-vetting-operations-support-bpa/. On April 9, 2019, Amyx's protest was denied. Government Accountability Office, "Matter of Amyx, Inc.," file B-416734.2, April 9, 2019, https://www.gao.gov/assets/700/698548.pdf.

364 DHS Contract with SRA International, August 19, 2018—August 19, 2023, USASpending, https://www.usaspending.gov/#/award/68975297.

365 *See supra* text accompanying notes 18-24 and *infra* text accompanying notes 438-441.

366 DHS, Privacy Impact Assessment for the Immigration and Customs Enforcement Forensic Analysis of Electronic Media, DHS/ICE/PIA-042, May 11, 2015 (hereinafter ICE Forensic Analysis of Electronic Media 2015 PIA), 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-forensicanalysisofelectronicmedia-may2015.pdf.

367 Thomas Brewster, "US Immigration Splurged $2.2 Million on Phone Hacking Tech Just After Trump's Travel Ban," *Forbes*, April 13, 2018, https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/#16764176a1fc.

368 The total ICE has spent on UFEDs since 2009 is at least $4,289,048. ICE contracts with Cellebrite, February 2, 2009–April 25, 2018, "Spending by Prime Award," USASpending, https://www.usaspending.gov/#/search/15e82c94e158f05fd85038b24821b92f. According to a forensics community source interviewed by *Forbes,* one UFED unit sells for between $5,000 and $15,000. Thomas Brewster, "US Immigration Splurged $2.2 Million on Phone Hacking Tech Just After Trump's Travel Ban." Not all of the money is spent on actual physical devices, however; some of the funds go to "annual license renewals." *See* ICE contract with Cellebrite, April 25, 2018–August 15, 2018, USASpending, https://www.usaspending.gov/#/award/65728721.

369 ICE/CBP Electronic Device Searches 2009 PIA, 18.

370 *See supra* text accompanying notes 142-148.

371 ICE 2009 Directive, Border Searches of Electronic Devices, 2.

372 Documents note that searches should "to the extent practicable" be conducted in the presence of or with knowledge of the traveler. As with CBP, this is sometimes not practicable due to law enforcement, national security, or other concerns. Ibid.

373 ICE/CBP Electronic Device Searches 2009 PIA, 3; Act of August 4, 1790, 1 Stat. 164.

374 ICE claims that electronic devices are equally subject to search because "the information contained in them may be relevant to DHS's customs and immigration inspection processes and decisions." ICE/CBP Electronic Device Searches 2009 PIA, 3.

375 *Riley v. California*, 134 S. Ct. 2473, 2488 (2014).

376 ICE 2009 Directive, Border Searches of Electronic Devices, 5. If detained longer, they require supervisory approval every 15 days thereafter. Ibid.

377 ICE/CBP Electronic Device Searches 2009 PIA, 8.

378 The sole example given is that of a traveler who appears to be permitted legal entry as a visitor, but whose laptop contains a file revealing evidence of his "true intent to secure employment" in the United States, "making him inadmissible." Ibid., 5.

379 Ibid., 5. Notes from the search process can be kept for as long as allowed by the retention schedule of the system the notes are stored in. Ibid., 19. *See* also DHS Privacy Office, Notice of Privacy Act System of Records, ICE– 006 Intelligence Records System of Records, 75 Fed. Reg. 9233, 9235 (March 1, 2010) (hereinafter IIRS SORN), https://www.federalregister.gov/d/2010-4102/p-3.

380 ICE 2009 Directive, Border Searches of Electronic Devices, 7. CBP and ICE have 76 Customs Mutual Assistance Agreements to share information with foreign customs partners in support of specific cases. CBP, "DHS Transition Issue Paper: International Information Sharing," in *CBP Presidential Transition Records*, 2.

381 ICE/CBP Electronic Device Searches 2009 PIA, 9. According to the ICE directive, information shared with assisting agencies is retained only for the amount of time necessary to provide assistance and is generally returned or destroyed upon completion. However, an assisting federal agency may retain a copy if it has the independent legal authority to do so (e.g., when the information has "national security or intelligence value"). ICE 2009 Directive, Border Searches of Electronic Devices, 8.

382 Memorandum from director, ICE Office of Investigations, to assistant directors et al., "Field Guidance on Handling Detained or Seized Electronic Media," 2. There are few details available about ICE's auditing mechanisms for its border searches; we know only that the agency conducts regular "self-assessments" to "verify compliance with its responsibilities." ICE/CBP Electronic Device Searches 2009 PIA, 25. While ICE is meant to develop and "periodically administer" an auditing mechanism to assess whether border searches of electronic devices are being conducted in line with its directive, it is not known whether the agency has done so. *See* ICE 2009 Directive, Border Searches of Electronic Devices, 10.

383 ICE has legal authority to issue subpoenas, summonses, and Form I-9 notices through 50 U.S.C. App. § 2411(a) for the Export Subpoena, 21 U.S.C. § 967 for the Controlled Substance Enforcement Subpoena, 19 U.S.C. § 1509 for the Customs Summons, Immigration and Nationality Act (INA) § 235(d)(4)(A) for the Immigration

Subpoena, and INA § 274A(e)(2)(C) for the Form I-9 notice. DHS, Privacy Impact Assessment for the ICE Subpoena System, March 29, 2011, https://www.dhs.gov/sites/default/files/publications/privacy_pia_27_ice_iss.pdf. For example, ICE can subpoena witness testimony before immigration officers and the production of books, papers, and documents "relating to the privilege of any person to enter, reenter, reside in, or pass through the United States or concerning any matter which is material and relevant to the enforcement of this Act and the administration of the Service." INA § 235(d)(4)(A).

384 ICE Forensic Analysis of Electronic Media 2015 PIA, 5, 6. Agents use a variety of electronic tools to collect and comb through electronic media and extract "relevant evidentiary material." For example, certain tools make digital images of the media, create a mirror copy to use as the working copy, and index and extract files and other data points. Some require an agent to create index terms for search purposes, whereas others have terms that are predetermined "based on the common type of data found in electronic media." Ibid., 2. The 2015 privacy impact assessment does not list any tools by name, noting only that multiple tools may be used on a single device. Ibid., 6. However, given that ICE has purchased UFEDs, which are designed for these types of functions, it is likely that they are used throughout HSI operations involving electronic media, during investigations as well as border searches. *See supra* text accompanying notes 134-135 and 367-368.

385 Ibid., 5.

386 Ibid., 2.

387 For cases that do not result in prosecution, the original digital evidence is retained until the case is closed, unless the evidence is required for follow-up investigation, in which case it is retained for 16 years. For open cases where there is no statute of limitations for the crime, the original digital evidence is considered a permanent record and preserved indefinitely. Ibid., 8.

388 Ibid., 9.

389 According to the privacy impact assessment, "the information may be further disseminated by recipients on a need-to-know basis in order to ensure proper investigation and prosecution of criminal violations. If evidence of a potential law violation is extracted from digital media, it may be used as necessary by the recipient to carry out its law enforcement functions, including prosecution of the violation. This could involve re-dissemination to others whose input is needed." Ibid., 9-10.

390 Ibid., 1.

391 Ibid., 2. Some of the tools are "government off-the-shelf applications," whereas others are developed specifically for and purchased by ICE. Ibid.

392 Ibid., 7.

393 IIRS SORN, 9235.

394 FALCON-SA 2016 PIA, 32; ICE, "Social Network Analysis: Advanced Reference Guide," 1, https://epic.org/foia/dhs/ice/palantir-databases/FALCON-Social-Network-Analysis-Reference-Guide.pdf.

395 FALCON-SA contains information on various categories of individuals, such as those who are the subject of investigations or border encounters with DHS or individuals associated with tips concerning criminal or suspicious activity. FALCON-SA 2016 PIA, 4. FALCON-SA records may include some or all of the following types of personally identifiable information: identifying and biographic data, citizenship and immigration data, customs import-export history, criminal history, contact information, criminal associations, family relationships, employment, military service, education, and other background information. Ibid.

396 DHS Management Directorate, "DHS Lexicon Terms and Definitions," 473 (defining *pattern analysis*).

397 FALCON-SA 2016 PIA, 2-3.

398 Users can add social media information to FALCON-SA either to "verify or update information already in the system" or "to add other information about an individual that is not available in FALCON-SA" already. DHS, Privacy Impact Assessment Update for the FALCON Search & Analysis System, DHS/ICE/PIA-032(a), January 16, 2014, 10, https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf. "Open-source data," which includes social media information, is listed as a category of data that can be uploaded into FALCON-SA on an ad hoc basis. FALCON-SA 2016 PIA, 35.

399 Lookout records are based on law enforcement, anti-terrorism, travel document fraud, or other interests based on previous violations of law or suspicion of violations. CBP officers use lookout records at primary and secondary inspection processing at the ports of entry. *See* DHS, Privacy Impact Assessment for the TECS System: Platform, DHS/CBP/PIA-021, August 12, 2016, 12, https://www.dhs.gov/sites/default/files/publications/DHS-PIA-ALL-021%20TECS%20System%20Platform.pdf.

400 CBP and ICE both use TECS for lookout records, and TECS stores records of electronic device searches, which may be included in lookout records. OIG 2018 Electronic Device Report, 4.

401 FALCON-SA 2016 PIA, 32-33.

402 Other data sources in FALCON-SA include ad hoc uploads of criminal history information and warrant or other lookout records from domestic and foreign law enforcement sources, including the FBI's National Crime Information Center (NCIC); finished intelligence reports generated by DHS and other law enforcement or intelligence agencies; and information or reports supplied by foreign governments and multinational organizations. FALCON-SA 2016 PIA, 35-6. Passenger Name Record (PNR) data obtained from ATS may not be uploaded or entered into FALCON-SA. Ibid., 35.

403 For instance, telecommunications records could be helpful in providing additional information about one's "social network." According to 2013 DHS funding documents that the *Intercept* obtained via FOIA request, FALCON-SA allows users "to follow target telephone activity and GPS movement on a map in real time." DHS, "FALCON New Requirements for Outline," 2013, 5, https://www.documentcloud.org/documents/3517286-FALCON-New-Requirements-Outline.html#document/p1. See also Spencer Woodman, "Palantir Enables Immigration Agents to Access Information From the CIA," *Intercept*, March 17, 2017, https://theintercept.com/2017/03/17/palantir-enables-immigration-agents-to-access-information-from-the-cia/.

404 FALCON-SA 2016 PIA, 2.

405 DHS Privacy Office, Notice of Proposed Rulemaking, ICE–016 FALCON Search and Analysis System of Record, 82 Fed. Reg. 20844, 20846 (May 4, 2017), https://www.regulations.gov/document?D=DHS_FRDOC_0001-1573.

406 The following types of information from IIRS are ingested by FALCON-SA: "law enforcement, intelligence, crime, and incident reports, and reports of suspicious activities, threats, or other incidents generated by ICE and other agencies." FALCON-SA 2016 PIA, 32. ICE's Office of Intelligence manages IIRS. IIRS SORN, 9233.

407 IIRS SORN, 9235.

408 Ibid. The ICE Intelligence Records System maintains records to produce intelligence reports that provide actionable information to ICE personnel and other government agencies. Ibid.

409 All information that may help establish patterns of unlawful activity is retained, whether relevant or necessary to an investigation. DHS Privacy Office, Final Rule, ICE–006 Intelligence Records System, 75 Fed. Reg. 12437, 12438 (March 16, 2010), http://www.gpo.gov/fdsys/pkg/FR-2010-03-16/pdf/2010-5618.pdf. Other records in the system include terrorist watch list information; records pertaining to known or suspected terrorists, terrorist incidents, activities, groups, and threats; intelligence reporting from other groups or agencies; and suspicious activity and threat reports from ICE and outside entities. IIRS SORN 9235, 9237.

410 FALCON-SA 2016 PIA, 2, 32-3.

411 Ibid., 2-3.

412 ICE, "Social Network Analysis: Advanced Reference Guide," 1, https://epic.org/foia/dhs/ice/palantir-databases/FALCON-Social-Network-Analysis-Reference-Guide.pdf.

413 Potential ERO access to the system is not addressed in FALCON-SA privacy impact assessments or system of records notices. FALCON-SA 2016 PIA; DHS, System of Records Notice, FALCON-Search and Analysis System of Records, 82 Fed. Reg. 20905 (May 4, 2017), https://www.regulations.gov/contentStreamer?documentId=DHS-2017-0001-0001&contentType=pdf. However, HSI can share information from FALCON-SA with ERO on a need-to-know basis. Ibid., 20906. *See* also Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine" (noting that ICE did not respond to questions about whether FALCON is made available to ERO agents).

414 Other FALCON modules include FALCON Data Analysis and Research for Trade Transparency (DARTTS) and the FALCON Roadrunner System. FALCON-SA 2016 PIA, 34; DHS, Privacy Impact Assessment for the FALCON-Roadrunner DHS/ICE/PIA-040, November 12, 2014, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-falconroadrunner-november2014.pdf.

415 Electronic Privacy Information Center, FOIA Request Letter to Pavlik-Keenan, 1-2; *see* alsoWoodman, "Palantir Enables Immigration Agents to Access Information From the CIA."

416 Homeland Security Investigations Mission Support, "FALCON Operations & Maintenance Support & System Enhancement, Performance Work Statement," 16.

417 ICE contract with Palantir Technologies Inc., "FALCON Operations and Maintenance (O&M) Support Services and Optional Enhancements," November 28, 2018–November 27, 2019, USASpending, https://www.usaspending.gov/#/award/75332582. In May 2018, Palantir concluded a three-year contract for work on FALCON worth $39 million. ICE contract with Palantir Technologies Inc., "FALCON Operations and Maintenance (O&M), System Enhancement Support Services for Palantir Government," May 28, 2015–May 27, 2018, USASpending, https://www.usaspending.gov/#/award/23844369. *See* also earlier contract for FALCON work, ICE contract with Palantir Technologies Inc., "FALCON Operations and Maintenance (O&M) Support Services," June 14, 2013–May 27, 2015, USASpending, https://www.usaspending.gov/#/award/23843927. Between June 7 and 18, 2018, Palantir completed a $250,000 contract with ICE for "Palantir Gotham Software," likely for FALCON software upgrades. ICE contract with Palantir Technologies Inc., "Palantir Gotham Software," June 7–18, 2018, USASpending, https://www.usaspending.gov/#/award/66572630.

418 FDNS 2014 PIA, 1-2.

419 Ibid., 1. Other USCIS directorates, such as the Field Operations Directorate, are also "exploring" social media as an added vetting tool. Citizenship and Immigration Services Ombudsman, *Annual Report 2018,* June 28, 2018 (hereinafter USCIS 2018 Annual Report), 34, https://www.dhs.gov/sites/default/files/publications/DHS%20Annual%20Report%202018.pdf.

420 USCIS 2018 Annual Report, 34.

421 Hearing on Refugee Admissions: Cissna Testimony, 5; USCIS 2018 Annual Report, 34.

422 Office of Inspector General, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success*, 8; USCIS Briefing Book, 180.

423 USCIS 2018 Annual Report, 34.

424 Hearing on Refugee Admissions: Cissna Testimony, 5.

425 Rex W. Tillerson, Elaine Duke, and Daniel Coats, Memorandum to the President, "Resuming the United States Refugee Admissions Program With Enhanced Vetting Capabilities," October 23, 2017, 2, https://www.dhs.gov/sites/default/files/publications/17_1023_S1_Refugee-Admissions-Program.pdf.

426 Exec. Order No. 13,780, 82 Fed. Reg. 13209 (March 6, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-03-09/pdf/2017-04837.pdf.

427 Laura Koran and Tal Kopan, "US Increases Vetting and Resumes Processing of Refugees From 'High-Risk' Countries."

428 *See* USCIS, *Review of the Defense Advanced Research Projects Agency 2.0 Social Media Pilot*, June 2, 2016, 9, https://www.documentcloud.org/documents/4341532-COW2017000400-FOIA-Response.html#document/p1; USCIS Briefing Book, 181.

429 DHS, Privacy Impact Assessment for the Refugee Case Processing and Security Vetting, DHS/USCIS/PIA-068, July 21, 2017 (hereinafter USCIS 2017 Refugee Vetting PIA), 5, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf. The U.S. Refugee Admissions Program is the program charged with vetting the entry of and resettling eligible refugees to the United States. Although the Department of State is the overall manager, the program is jointly run with USCIS. Ibid., 1. FDNS is responsible for conducting social media checks on refugee applicants. Ibid., 7.

430 Ibid., 7.

431 Ibid. The prohibition on interacting with applicants, however, still applies during masked monitoring. Ibid., 8.

432 León Rodriguez, USCIS director, to Sarah M. Kendall, associate director, Fraud Detection and National Security, and Joseph E. Langlois, associate director, Refugee, Asylum and International Operations, "Fraud Detection and National Security Use of Social Media for Refugee Processing," April 7, 2015, https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf#page=1442.

433 USCIS 2017 Refugee Vetting PIA, 18.

434 USCIS Briefing Book, 183.

435 Ibid.

436 DHS, Privacy Impact Assessment for the USCIS Asylum Division, DHS/USCIS/PIA-027(C), July 21, 2017 (hereinafter USCIS 2017 Asylum Division PIA), 20, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-asylum-july2017_0.pdf.

437 USCIS 2017 Asylum Division PIA, 20-21.

438 USCIS Briefing Book, 183.

439 USCIS, "USCIS Social Media & Vetting: Overview and Efforts to Date," 3.

440 Ibid.

441 Office of Inspector General, *DHS' Pilots for Social Media Screening Need Increased Rigo*r, 1, 6.

442 USCIS 2017 Refugee Vetting PIA, 2.

443 The "clear" and "not clear" designations are applied to the date of the background check, whether the check found any derogatory results, whether the results were resolved, and the expiration date of the results. USCIS 2017 Refugee Vetting PIA, 9.

444 A-Files SORN, 43556.

445 Ibid., 43557.

446 Ibid.

447 Matt Novak, "US Homeland Security Says Tracking Social Media of Immigrants Is Nothing New," *Gizmodo*, September 28, 2017, https://gizmodo.com/us-homeland-security-says-tracking-social-media-of-immi-1818875395.

448 USCIS, *Review of the Defense Advanced Research Projects Agency 2.0 Social Media Pilot*, 57; Jonathan R. Scharfen, deputy director, USCIS, to field leadership, "Policy for Vetting and Adjudicating Cases With National Security Concerns," 1, April 11, 2008, (hereinafter CARRP Policy for Vetting and Adjudicating Cases With National Security Concerns), https://www.uscis.gov/sites/default/files/USCIS/About%20Us/Electronic%20Reading%20Room/Policies_and_Manuals/CARRP_Guidance.pdf.

449 *See*, for example, Jennie Pasquarella, *Muslims Need Not Apply: How USCIS Secretly Mandates Discriminatory Delays and Denials of*

Citizenship and Immigration Benefits to Aspiring Americans, ACLU of Southern California, August 2013, 1, https://www.aclusocal.org/sites/default/files/carrp-muslims-need-not-apply-aclu-socal-report.pdf. The CARRP policy applies to "all applications and petitions that convey immigrant and nonimmigrant status." CARRP Policy for Vetting and Adjudicating Cases With National Security Concerns, 1. The ACLU of Southern California has further clarified that this includes individuals applying for asylum, visas, green cards, and naturalization. Pasquarella, *Muslims Need Not Apply,* 9.

450 Pasquarella, *Muslims Need Not Apply*, 2-3.

451 *Wagafe v. Trump*, No. C17-0094-RAJ, 2017 WL 2671254, at *1 (W.D. Wash. June 21, 2017).

452 USCIS Briefing Book, 182.

453 National Counterterrorism Center, "Watchlisting Guidance," 10. For more information on this watch list and the privacy and civil liberties issues associated with it, *see supra* text accompanying notes 267-273.

454 Pasquarella, *Muslims Need Not Apply*, 17.

455 Ibid.

456 According to the CARRP definition, a national security concern arises when "an individual or organization has been determined to have an articulable link to prior, current, or planned involvement in, or association with, an activity, individual or organization described in [the security and terrorism sections] of the Immigration and Nationality Act." CARRP Policy for Vetting and Adjudicating Cases With National Security Concerns, 1n1. However, the looseness of terms used in the definition — e.g., "articulable link," which can be attenuated or unsubstantiated, and "association," which can be distant or marginal — means that the government has extensive leeway to place someone on the CARRP list. Amended Complaint for Declaratory and Injunctive Relief, *Wagafe v. Trump* (W.D. Wash. Feb. 1, 2017), https://www.aclu.org/legal-document/wagafe-v-uscis-amended-complaint. *See* also Katie Traverso and Jennie Pasquarella, "Practice Advisory: USCIS's Controlled Application Review and Resolution Program," 3, https://www.nationalimmigrationproject.org/PDFs/practitioners/our_lit/impact_litigation/2017_03Jan-ACLU-CARRP-advisory.pdf.

457 A guidance states that in "Family Member or Close Associate" cases, officers must determine "if the [national security] concern relates to the individual, and if so, if it gives rise to a [national security] concern for the individual." USCIS, "CARRP Officer Training," April 2009, 5, https://www.aclusocal.org/sites/default/files/wp-content/uploads/2013/01/Guiance-for-Identifying-NS-Concerns-USCIS-CARRP-Training-Mar.-2009.pdf.

458 DHS, Privacy Impact Assessment for the Fraud Detection and National Security Data System (FDNS-DS), DHS/USCIS/PIA-013(a) May 18, 2016 (hereinafter FDNS-DS 2016 PIA), 14, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-fdnsds-november2017.pdf. Commercial and public sources may be used to verify information provided by the individual, support or refute signs of fraud, and identify public safety or national security concerns. Ibid.

459 "DHS Operational Use of Social Media," 8, in USCIS Briefing Book, 141; Ibid., 137.

460 "DHS Operational Use of Social Media," 8, in USCIS Briefing Book, 141. The other USCIS programs that require updated privacy impact assessments to reflect the use of social media include Computer Linked Application Information Management System (CLAIMS) 3; CLAIMS 4; and Refugees, Asylum, and Parole System and the Asylum Pre-Screening System (RAPS/APSS). CLAIMS 3 manages the adjudication process for most domestically filed, paper-based immigration benefit filings with the exception of naturalization; intercountry adoption; and certain requests for asylum and refugee status. DHS, Privacy Impact Assessment Update for the Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, DHS/USCIS/PIA-016(a), March 25, 2016, 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-claims3appendixaupdate-may2018.pdf. CLAIMS 4 tracks and processes naturalization applications. DHS, Privacy Impact Assessment Update for the Computer Linked Application Information Management System 4 (CLAIMS 4), DHS/USCIS/PIA-015(b), November 5, 2013, 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-update-uscis-claims4-november2013.pdf.

461 Privacy Impact Assessment for the Continuous Immigration Vetting, DHS/USCIS/PIA-076, February 14, 2019 (hereinafter USCIS CIV 2019 PIA), 2, https://www.dhs.gov/sites/default/files/publications/pia-uscis-fdnsciv-february2019_0.pdf.

462 Ibid., 6.

463 Ibid., 7.

464 Like CARRP, the Continuous Immigration Vetting privacy impact assessment considers a "national security concern" to arise when "an individual or organization has been determined to have an articulable link to prior, current, or planned involvement in, or association with, an activity, individual or organization described in [the security and terrorism sections] of the Immigration and Nationality Act." Ibid.

465 Ibid., 8.

466 ATLAS is built into the USCIS system FDNS-DS, which is the main database that FDNS officers use to manage the background check process related to immigration applications and petitions, and information related to applicants with suspected or confirmed fraud, criminal activity, public safety or national security concerns, and cases randomly selected for benefit fraud assessments. FDNS 2014 PIA, 6.

467 FDNS-DS 2016 PIA, 3.

468 Ibid., 5-6. As of May 2016, USCIS was incorporating new capabilities into ATLAS, including predictive analytics, link and forensic analysis, and other analytic functions. Ibid., 6.

469 USCIS CIV 2019 PIA, 7.

470 Ibid.

471 Ibid., 18.

472 FDNS 2014 PIA, 38.

473 Ibid., 4.

474 FDNS-DS 2016 PIA, 4.

475 FDNS 2014 PIA, 6.

476 FDNS-DS 2016 PIA, 14. The privacy impact assessment also states that information found in open sources may be provided by FDNS to USCIS adjudications personnel to formulate a request for additional evidence when an immigration application or a petitioner lacks required documentation, to draft a notice when an individual is found ineligible for asylum, or to use during an interview with a petitioner or beneficiary in order to discuss any derogatory information that may have been found. FDNS 2014 PIA, 6. See USCIS, *Adjudicator's Field Manual,* Chapter 10.5, "Requesting Additional Information," https://www.uscis.gov/ilink/docView/AFM/HTML/AFM/0-0-0-1/0-0-0-1067/0-0-0-1318.html; USCIS, "Types of Asylum Decisions," accessed March 26, 2019, https://www.uscis.gov/humanitarian/refugees-asylum/asylum/types-asylum-decisions.

477 According to a 2008 internal FDNS memo, "social networking gives FDNS an opportunity to reveal fraud by browsing these sites to see if petitioners and beneficiaries are in a valid relationship or are attempting to deceive CIS about their relationship." USCIS, "Social Networking Sites and Their Importance to DHS," May 2008, 1, https://www.eff.org/files/filenode/social_network/dhs_customsimmigration_socialnetworking.pdf.

478 FDNS 2014 PIA, 6.

479 FDNS-DS 2016 PIA, 15.

480 FDNS 2014 PIA, 5.

481 ATS 2017 PIA, 14, 43; DHS Privacy Office, Notice of Privacy Act System of Records, CBP–006 Automated Targeting System, System of Records, 77 Fed. Reg. 30297 (May 22, 2012), https://www.govinfo.gov/content/pkg/FR-2012-05-22/pdf/2012-12396.pdf.

482 ATS 2017 PIA, 14.

483 ESTA 2016 PIA, 5.

484 Ibid., 6.

485 ESTA SORN, 60717.

486 AFI 2012 PIA, 9.

487 Ibid., 18.

488 CIRS SORN, 44202.

489 CBP 2018 Digital Forensics PIA, 7. Information obtained through a search warrant that is subsequently found to be outside the scope of that warrant will be deleted from the system once the case or trial is complete. Ibid., 5.

490 Secure Flight 2017 PIA, 9.

491 ATS 2017 PIA, 25-6.

492 Silent Partner and Quiet Skies 2019 PIA, 11-12.

493 Ibid., 25.

494 Secure Flight 2017 PIA, 9.

495 An exception to the time frame for remaining on the ineligible list is if the crime disqualifying an applicant is time-limited. For example, some offenses may not be disqualifying if the application is made more than seven years after conviction. PreCheck 2016 PIA, 9.

496 PreCheck 2013 PIA, 7.

497 Ibid.

498 Ibid.

499 However, ICE has stated that it intends to request approval from NARA to reduce the retention period to 25 years from the date the record was created. LeadTrac 2016 PIA, 15. If ICE's request is approved, records would be "active" for 20 years and then archived for 5 years. After this 25-year period, records would be destroyed or retained further "under a reset retention schedule" if deemed necessary. Ibid., 25.

500 ICM 2016 PIA, 28.

501 Ibid., 29.

502 Visualizations and search queries containing personally identifiable information but without an associated case number must be recertified annually by the user or supervisor, or the information is purged from the system. FALCON-SA 2014 PIA, 18.

503 Ibid., 35.

504 IIRS SORN, 9237.

505 A-Files SORN, 43564.

506 FDNS-DS 2016 PIA, 8.

507 The DHS Data Framework was originally intended to enforce data retention restrictions by relying on the source systems to notify the Data Framework of changes, deletions, or corrections to data. However, the privacy impact assessment notes that source systems have not adequately notified the Data Framework, leading to inconsistent compliance with source systems' data retention rules. DHS, Privacy Impact Assessment for DHS Data Framework — Retention, DHS/ALL/PIA-046(d), March 15, 2017, 1-2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-all-046-d-dhsdata-frameworkretention-march2017.pdf.

Graphic icons on pages 17, 19-21, and 28: Created by sahua d, Delwar Hossain, Marla Ambrosetti, and Diego Naive of the Noun Project.

Endnotes for Sidebars

Case Studies: Using Social Media to Target First Amendment–Protected Activity

i Jimmy Tobias, "Exclusive: ICE Has Kept Tabs on 'Anti-Trump' Protesters in New York City," *The Nation*, March 6, 2019, https://www.thenation.com/article/ice-immigration-protest-spreadsheet-tracking/.

ii Ibid.

iii Tom Jones, Mari Payton, and Bill Feather, "Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database," NBC San Diego, March 6, 2019, https://www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html.

iv Ibid.

v Bennie Thompson and Kathleen Rice to CBP Commissioner Kevin McAleenan, March 7, 2019, https://homeland.house.gov/sites/democrats.homeland.house.gov/files/documents/190307McAleen.pdf.

vi Ryan Devereaux, "Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests," *Intercept,* April 29, 2019, https://theintercept.com/2019/04/29family-separation-protests-surveillance/.

vii Ibid.

Automated Extreme Vetting

i *See*, for example, Morgan Chalfant, "Tech Experts Blast Trump's Extreme Vetting Plan," *The Hill*, November 16, 2017, https://thehill.com/policy/cybersecurity/360664-tech-experts-blast-trumps-extreme-vetting-plan.

ii Exec. Order No. 13,769, 82 Fed. Reg. 8977 (January 27, 2017), https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states/.

iii *International Refugee Assistance Project v. Trump*, 857 F.3d 554 (4th Cir.), http://coop.ca4.uscourts.gov/171351.P.pdf. *See* ICE, "Extreme Vetting Initiative: Statement of Objectives (SOO)," http://www.brennancenter.org/sites/default/files/Extreme%20Vetting%20Inititate%20-%20Statement%20of%20Objectives.pdf; ICE, "Attachment 2: Background," ICE-HSI — Data Analysis Service Amendment, Solicitation No. HSCEMD-17-R-00010, *GovTribe*, June 12, 2017, http://www.brennancenter.org/sites/default/files/Extreme%20Vetting%20Inititate%20-%20Statement%20of%20Objectives.pdf.

iv Hal Abelson et al. to Acting Secretary of Homeland Security Elaine C. Duke, November 16, 2017, https://www.brennancenter.org/sites/default/files/Technology%20Experts%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%2011.15.17.pdf.

v Ibid.

vi Cedric Richmond, Bennie Thompson, and Yvette Clarke to Acting Secretary of Homeland Security Kirstjen Nielsen, March 8, 2018, https://www.brennancenter.org/sites/default/files/analysis/CBC%20DHS%20Letter%20re%20Extreme%20Vetting_1.pdf/.

vii Drew Harwell and Nick Miroff, "ICE Just Abandoned Its Dream of 'Extreme Vetting' Software That Could Predict Whether a Foreign Visitor Would Become a Terrorist," *Washington Post*, May 17, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/?utm_term=.57cbc2fc8442.

ABOUT THE AUTHORS

▶ **Faiza Patel** serves as co-director of the Brennan Center's Liberty and National Security Program. She has testified before Congress opposing the dragnet surveillance of Muslims, developed legislation to create an independent inspector general for the New York Police Department, and organized advocacy efforts against anti-Muslim laws and policies. She has authored or co-authored eight reports: *Extreme Vetting and the Muslim Ban* (2017), *Trump-Russia Investigations: A Guide* (2017), *The Islamophobic Administration* (2017), *Countering Violent Extremism* (2017), *Overseas Surveillance in an Interconnected World* (2016), *What Went Wrong With the FISA Court* (2015), *Foreign Law Bans* (2013), *A Proposal for an NYPD Inspector General* (2012), and *Rethinking Radicalization* (2011). She is a member of the Board of Editors of the legal blog Just Security. Born and raised in Pakistan, Patel is a graduate of Harvard College and the NYU School of Law.

▶ **Rachel Levinson-Waldman** is senior counsel in the Brennan Center's Liberty and National Security Program, where she works to shed light on the use of monitoring and surveillance technologies by the federal government as well as by state and local law enforcement. Ms. Levinson-Waldman has authored essays on law enforcement surveillance of social media in the *Oklahoma Law Re*view (2019) and *Howard Law Review* (2018), authored an article on the Fourth Amendment and government surveillance in public in the *Emory Law Revie*w (2017), and authored or co-authored the following Brennan Center reports and white papers: *Cellphones, Law Enforcement, and the Right to Privac*y (2018), *Trump-Russia Investigations: A Guide* (2017), *The Islamophobic Administrati*on (2017), and *What the Government Does With Americans' Data* (2013). She is a graduate of Williams College and the University of Chicago Law School.

▶ **Raya Koreh** is a research and program associate in the Liberty and National Security Program at the Brennan Center for Justice. At the Brennan Center, her work has focused on issues surrounding surveillance, religious and racial profiling, and online civil rights and civil liberties. She graduated summa cum laude and Phi Beta Kappa from Harvard College in May 2018 with an undergraduate degree in history.

▶ **Sophia DenUyl** is the special assistant to the co-directors of the Liberty and National Security Program, where she works on issues related to digital surveillance and racial and religious profiling, and provides programmatic support. Sophia graduated with honors from Barnard College in May 2017 with a B.A. in political science and a minor in Spanish & Latin American cultures.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect constitutional values and the rule of law, using research, innovative policy recommendations, litigation, and public advocacy. The program focuses on reining in excessive government secrecy, ensuring that counterterrorism authorities are narrowly targeted to the terrorist threat, and securing adequate oversight and accountabil- ity mechanisms.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges The Bauman Foundation, Democracy Alliance Partners, Ford Foundation, Media Democracy Fund, Open Society Foundations, and Rockefeller Brothers Fund for their support of our liberty and national security work.

The authors would like to express their gratitude to the Brennan Center's Lorraine Cademartori, Mireya Navarro, Stephen Fee, Jeanne Park, Yuliya Bas, Lisa Benenson, and Alden Wallace for their editing and communications assistance, to Harsha Panduranga for his review and drafting contributions, and to Andrew Lindsay for his research contributions. We appreciate the guidance and support of Michael Waldman and John Kowal. They also thank Manar Waheed, Esha Bhandari, Edward Hasbrouck, Jeramie Scott, and Bruce Friedman for their invaluable review and subject matter expertise.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway | 17th Floor | New York, NY 10271
www.brennancenter.org